§ 115C-402.5. Student data system security.

(a) Definitions. – The following definitions apply in this section:

(1) Aggregate student data. – Data collected or reported at the group, cohort, or institutional level.

(2) De-identified student data. – A student dataset in which parent and student personal or indirect identifiers, including the unique student identifier, have been removed.

(3) FERPA. – The federal Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

(4) Personally identifiable student data. – Student data that:

a. Includes, but is not limited to, the following:

1. Student name.
2. Name of the student's parent or other family members.
3. Address of the student or student's family.
4. Personal identifier, such as the student's Social Security number or unique student identifier.
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
7. Information requested by a person who the Department of Public Instruction or local school administrative unit reasonably believes knows the identity of the student to whom the education record relates.

b. Does not include directory information that a local board of education has provided parents with notice of and an opportunity to opt out of disclosure of that information, as provided under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, unless a parent has elected to opt out of disclosure of the directory information.

(5) Student data system. – The student information management system used by the State Board of Education and Department of Public Instruction as part of the Uniform Education Reporting Systems for collection and reporting of student data from local boards of education.

(b) Security of Student Data System. – To ensure student data accessibility, transparency, and accountability relating to the student data system, the State Board of Education shall do all of the following:

(1) Create and make publicly available a data inventory and index of data elements with definitions of individual student data fields in the student data system, including, but not limited to:

a. Any personally identifiable student data required to be reported by State and federal education mandates.

b. Any other individual student data which has been proposed for inclusion in the student data system, with a statement regarding the purpose or reason for the proposed collection.

(2) Develop rules to comply with all relevant State and federal privacy laws and policies that apply to personally identifiable student data in the student data system, including, but not limited to, FERPA and other relevant privacy laws and policies. At a minimum, the rules shall include the following:

a. Restrictions on access to personally identifiable student data in the student data system to the following individuals:

1. Authorized staff of the State Board of Education and Department of Public Instruction and the contractors working on behalf of the Department who require such access to perform their assigned duties.
2. Authorized North Carolina public school administrators, teachers, and other school personnel and contractors working on behalf of the board of the North Carolina public school who require such access to perform their assigned duties.
3. Students and their parents or legal guardians, or any individual that a parent or legal guardian has authorized to receive personally identifiable student data.
4. Authorized staff of other State agencies and contractors working on behalf of those State agencies as required by law and governed by interagency data-sharing agreements.

b. Criteria for approval of research and data requests for personally identifiable student data in the student data system made to the State Board of Education from State or local agencies, researchers working on behalf of the Department, and the public.

(3) Prohibit the transfer of personally identifiable student data in the student data system to individuals other than those identified in subdivision (2) of this subsection, unless otherwise permitted by law and authorized by rules adopted under this section. Such rules shall authorize the release of personally identifiable data out of State to schools or educational agencies when a student enrolls in a school out of State or a local school administrative unit seeks help with locating a student formerly enrolled in this State who is now enrolled out of State.

(4) Develop a detailed data security plan for the student data system that includes all of the following:

a. Guidelines for authorizing access to the student data system and to individual student data, including guidelines for authentication of authorized access.
b. Privacy compliance standards.
c. Privacy and security audits.
d. Breach planning, notification, and procedures.
e. Data retention and disposition policies.
f. Data security policies, including electronic, physical, and administrative safeguards such as data encryption and training of employees.

(5) Ensure routine and ongoing compliance by the Department of Public Instruction with FERPA, other relevant privacy laws and policies, and the privacy and security rules, policies, and procedures developed under the authority of this section related to personally identifiable student data in the

student data system, including the performance of compliance audits within the Department.

(6) Ensure that any contracts for the student data system that include de-identified student data or personally identifiable student data and are outsourced to private contractors include express provisions that safeguard privacy and security and include penalties for noncompliance.

(7) Notify the Governor and the General Assembly annually by October 1 of the following:

a. New student data, whether aggregate data, de-identified data, or personally identifiable student data, included or proposed for inclusion in the student data system for the current school year.

b. Changes to existing data collections for the student data system required for any reason, including changes to federal reporting requirements made by the United States Department of Education.

(c) Restricting on Student Data Collection. – The following information about a student or a student's family shall not be collected in nor reported as part of the student data system:

(1) Biometric information.

(2) Political affiliation.

(3) Religion.

(4) Voting history. (2014-50, s. 1.)