Education

§ 2-d. Unauthorized release of personally identifiable information. 1. Definitions. As used in this section the following terms shall have the following meanings:

a. "Building principal" means a building principal subject to annual performance evaluation review under the provisions of section three thousand twelve-c of this chapter.

b. "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of section three thousand twelve-c of this chapter.

c. "Educational agency" means a school district, board of cooperative educational services, school, or the education department.

d. "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

e. "School" means any public elementary or secondary school, universal pre-kindergarten program authorized pursuant to section thirty-six hundred two-e of this chapter, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in section four thousand one of this chapter, an approved private school for the education of students with disabilities, a state-supported school subject to the provisions of article eighty-five of this chapter, or a state-operated school subject to the provisions of article eighty-seven or eight-eight of this chapter.

f. "Student" means any person attending or seeking to enroll in an educational agency.

g. "Eligible student" means a student eighteen years or older.

h. "Parent" means a parent, legal guardian, or person in parental relation to a student.

i. "Student data" means personally identifiable information from student records of an educational agency.

j. "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of section three thousand twelve-c of this chapter.

k. "Third party contractor" shall mean any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to section two hundred eleven-e of this title and is not an educational agency as defined in paragraph c of this subdivision, and a not-for-profit corporation or other non-profit organization, other than an educational agency.

2. Chief privacy officer. a. The commissioner shall appoint a chief privacy officer within the department for a term of three years, which may be renewed for three-year terms thereafter. The chief privacy officer shall be qualified by training or experience in state and

federal education privacy laws and regulations, civil liberties, information technology, and information security. The chief privacy officer shall report to the commissioner on matters affecting privacy and the security of student, teacher, and principal data.

b. The functions of the chief privacy officer shall include, but not be limited to:

(1) promoting the implementation of sound information practices for privacy and security of student data or teacher or principal data;

(2) assisting the commissioner in handling instances of data breaches as well as assisting the commissioner in due process proceedings regarding any alleged breaches of student data or teacher or principal data;

(3) providing assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data or teacher or principal data;

(4) formulating a procedure within the department whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities the chief privacy officer determines is appropriate, may request information pertaining to student data or teacher or principal data in a timely and efficient manner;

(5) assisting the commissioner in establishing a protocol for the submission of complaints of possible breaches of student data or teacher or principal data;

(6) making recommendations as needed regarding privacy and the security of student data on behalf of the department to the governor, the speaker of the assembly, the temporary president of the senate, and the chairs of the senate and assembly education committees; and

(7) issuing an annual report on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to subparagraph five of this paragraph.

c. The chief privacy officer shall have the power to:

(1) access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by an educational agency that relate to student data or teacher or principal data;

(2) to review and comment upon any department program, proposal, grant, or contract that involves the processing of student data or teacher or principal data before the commissioner begins or awards the program, proposal, grant, or contract; and

(3) any other powers that the commissioner shall deem appropriate.

d. The chief privacy officer may hold more than one position within the department; provided, however, that no additional position may interfere with the duties of the chief privacy officer outlined in this paragraph.

3. Parents bill of rights for data privacy and security. a. A parents bill of rights for data privacy and security shall be published on the website of each educational agency and shall be included with every contract an educational agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data.

b. The parents bill of rights for data privacy and security shall state in clear and plain English terms that:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes;

(2) Parents have the right to inspect and review the complete contents of their child's education record;

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry

standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

(4) A complete list of all student data elements collected by the State is available for public review at (insert website address here) or by writing to (insert mailing address here); and

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to (insert phone number, email and mailing address here).

c. The parents bill of rights for data privacy and security shall include supplemental information for each contract an educational agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data. Such supplemental information shall be developed by the educational agency and shall include:

(1) the exclusive purposes for which the student data or teacher or principal data will be used;

(2) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

(3) when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

(4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

(5) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

d. The chief privacy officer, with input from parents and other education and expert stakeholders, shall develop additional elements of the parents bill of rights for data privacy and security. The commissioner shall promulgate regulations for a comment period whereby parents and other members of the public may submit comments and suggestions to the chief privacy officer to be considered for inclusion. The parents bill of rights for data privacy and security shall be completed within one hundred twenty days after the effective date of this section.

4. Data collection transparency and restrictions. a. The department shall promote the least intrusive data collection policies practicable that advance the goals of improving academic achievement, empowering parents with information and advancing efficient and effective school operations while minimizing the collection and transmission of personally identifiable information.

b. The chief privacy officer shall develop, regularly update and make publicly available on the department's website and through such additional methods as may facilitate accessibility an inventory and understandable description of the student, teacher and principal data elements collected with an explanation and/or legal or regulatory authority outlining the reasons such data elements are collected and the intended uses and disclosure of the data.

c. Except as otherwise specifically authorized by law, the department shall only collect personally identifiable information relating to an educational purpose.

d. The department may only require districts to submit personally identifiable information, including data on disability status and student suspensions, where such release is required by law or otherwise

authorized under the family educational rights and privacy act, 20 U.S.C. section 1232g, and the personal privacy protection law.

e. Except as required by law or in the case of educational enrollment data, school districts shall not report to the department the following student data elements:

(1) juvenile delinquency records;

(2) criminal records;

(3) medical and health records; and

(4) student biometric information.

f. Personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold or used for marketing purposes.

g. Parents shall have the right to inspect and review their child's educational record including any student data stored or maintained by an educational agency. The department shall develop policies for school districts that:

(1) provide for annual notification to parents of their right to request student data;

(2) ensure security when providing student data to parents, including that only authorized individuals receive such data; and

(3) specify a reasonable amount of time in which school districts should respond to such requests.

5. Data security and privacy standards. a. The commissioner, in consultation with the chief privacy officer, shall promulgate regulations establishing standards for educational agency data security and privacy policies and shall develop one or more model policies for use by educational agencies. The commissioner shall seek the input of experts, including those from security, cyber-security and fields in addition to education that have experience with personal data protection, in developing such standards and policies.

b. The standards for data security and privacy policies shall include, but not be limited to:

(1) data privacy protections, including criteria for determining whether a proposed use of personally identifiable information would benefit students and educational agencies, and processes to ensure that personally identifiable information is not included in public reports or other public documents;

(2) data security protections, including data systems monitoring, data encryption, incident response plans, limitations on access to personally identifiable information, safeguards to ensure personally identifiable information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of personally identifiable information when no longer needed; and

(3) application of all such restrictions, requirements and safeguards to third-party contractors.

c. Following promulgation of regulations by the commissioner pursuant to paragraph a of this subdivision each educational agency shall ensure that it has a policy on data security and privacy in place that is consistent with applicable state and federal laws and applied to student data and, where applicable, to teacher or principal data. Such policy shall be published on the educational agency's website, if it exists, and notice of such policy shall be provided to all officers and employees of the educational agency.

d. As applied to student data, such policy shall provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the family educational rights and privacy act, 20 U.S.C. section 1232g, where applicable the individuals with disabilities education act, sections fourteen hundred,

et seq. of title twenty of the United States code, and the federal regulations implementing such statutes. Each educational agency shall ensure that it has in place provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require that confidentiality of the shared student data or teacher or principal data be maintained in accordance with federal and state law and the educational agency's policy on data security and privacy.

e. Each educational agency that enters into a contract or other written agreement with a third party contractor under which the third party contractor will receive student data or teacher or principal data shall ensure that such contract or agreement includes a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy. Such plan shall include, but shall not be limited to, a signed copy of the parents bill of rights for data privacy and security, and a requirement that any officers or employees of the third party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

f. Each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data shall:

(1) limit internal access to education records to those individuals that are determined to have legitimate educational interests;

(2) not use the education records for any other purposes than those explicitly authorized in its contract;

(3) except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party:

(i) without the prior written consent of the parent or eligible student; or

(ii) unless required by statute or court order and the party provides a notice of the disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(4) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

(5) uses encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

6. Breach and unauthorized release of personally identifiable information. a. Each third party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement with an educational agency shall be required to notify such educational agency of any breach of security resulting in an unauthorized release of such data by the third party contractor or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of the educational agency and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The educational agency shall, upon notification by the third party

contractor, be required to report to the chief privacy officer any such breach of security and unauthorized release of such data. The chief privacy officer shall, upon belief that such breach and unauthorized release constitutes criminal conduct, report such breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

b. In the case of an unauthorized release of student data, the educational agency shall notify the parent or eligible student of the unauthorized release of student data that includes personally identifiable information from the student records of such student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized release of teacher or principal data, the educational agency shall notify each affected teacher or principal of the unauthorized release of data that includes personally identifiable information from the teacher or principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a parent, eligible student, teacher or principal under paragraph b of this subdivision due to the unauthorized release of student data by a third-party contractor or its assignee, the third-party contractor shall promptly reimburse the educational agency for the full cost of such notification.

d. Each violation of a third party contractor pursuant to paragraph a of this subdivision shall be punishable by a civil penalty of the greater of five thousand dollars or up to ten dollars per student, teacher, and principal whose data was released, provided that the latter amount shall not exceed the maximum penalty under paragraph (a) of subdivision six of section eight hundred ninety-nine-aa of the general business law.

e. If the chief privacy officer determines that a third party contractor or its assignee, in violation of applicable state or federal law, the data privacy and security policies of the educational agency provided by such educational agency to the third party contractor and/or binding contractual obligations relating to data privacy and security, has released any student data or teacher or principal data received from an educational agency to any person or entity not authorized by law to receive such data pursuant to a lawful subpoena or otherwise, the chief privacy officer, after affording the third party contractor with notice and an opportunity to be heard, shall be authorized to:

(1) order that the third party contractor be precluded from accessing student data or teacher or principal data, as applicable, from the educational agency from which the contractor obtained the data that was improperly disclosed for a fixed period of up to five years; and/or

(2) order that a third party contractor or assignee who knowingly or recklessly allowed for the unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years; and/or

(3) order that a third party contractor or assignee who knowingly or recklessly allowed for the unauthorized release of student data or teacher or principal data shall not be deemed a responsible bidder or offerer on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of the provisions of section one hundred three of the general municipal law or paragraph c of subdivision ten of section one hundred sixty-three of the state finance law, as applicable, for a fixed period of up to five years; and/or

(4) require the third party contractor to provide training at the contractor's expense on the federal and state law governing confidentiality of student data and/or teacher or principal data and the provisions of this section to all its officers and employees with access to such data, prior to being permitted to receive subsequent access to such data from the educational agency from which the contractor obtained the data that was improperly disclosed or from any educational agency; and/or

(5) if it is determined that the unauthorized release of student data or teacher or principal data on the part of the third party contractor or assignee was inadvertent and done without intent, knowledge, recklessness or gross negligence, the commissioner may determine that no penalty be issued upon the third party contractor.

7. Implementation and enforcement. a. The commissioner, in consultation with the chief privacy officer, shall promulgate regulations establishing procedures to implement the provisions of this section, including but not limited to procedures for the submission of complaints from parents and/or persons in parental relation to students, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal data by a third party contractor or its officers, employees or assignees that may be subject to the sanctions set forth in subdivision six of this section. Upon receipt of a complaint or other information indicating that such an improper disclosure by a third party contractor may have occurred, the chief privacy officer shall be authorized to investigate, visit, examine and inspect the third party contractor's facilities and records and obtain documentation from, or require the testimony of, any party relating to the alleged improper disclosure of student data or teacher or principal data.

b. Except as provided under paragraph d of subdivision six of this section, each violation of any provision of this section by a third party contractor or its assignee shall be punishable by a civil penalty of up to one thousand dollars; a second violation by the same third party contractor involving the same student data or teacher or principal data shall be punishable by a civil penalty of up to five thousand dollars; any subsequent violation by the same third party contractor involving the same student date or teacher or principal data shall be punishable by a civil penalty of up to ten thousand dollars. Each violation of this subdivision shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty under paragraph (a) of subdivision six of section eight hundred ninety-nine-aa of the general business law.

c. Nothing contained in this section shall be construed as creating a private right of action against the department or an educational agency.

d. Nothing in this section shall limit the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of an educational agency or of the state or any of its political subdivisions, any court or the federal government that is otherwise required by law.