ATTACHMENT A

AMENDMENT TO THE REGULATIONS OF THE COMMISSIONER OF EDUCATION

Pursuant to Education Law sections 2-d, 101, 207 and 305,

a new Part 121 shall be added effective upon adoption to read as follows:

Part 121

Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information

§121.1 Definitions.

As used in this Part, the following terms shall have the following meanings:

(a) *Breach* means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

(b) *Chief Privacy Officer* means the Chief Privacy Officer appointed by the Commissioner pursuant to Education Law §2-d.

(c) *Commercial or Marketing Purpose* means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.

(d) *Contract or other written agreement* means a binding agreement between an educational agency and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

(e) *Disclose* or *Disclosure* mean to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

(f) *Education Records* means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

(g) *Educational Agency* means a school district, board of cooperative educational services (BOCES), school, or the Department.

(h) *Eligible Student* means a student who is eighteen years or older.

(i) *Encryption means* methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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.

(j) *FERPA* means the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

(k) *NIST Cybersecurity Framework* means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

(l) *Parent* means a parent, legal guardian, or person in parental relation to a student.

(m) *Personally Identifiable Information*, as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of

Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in Education Law §3012-c (10).

(n) *Release* shall have the same meaning as Disclosure or Disclose.

(o) *School* means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, 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 Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law .

(p) *Student* means any person attending or seeking to enroll in an educational agency.

(q) *Student Data* means personally identifiable information from the student records of an educational agency.

(r) *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 Education Law §§3012-c and 3012-d.

(s) *Third-Party Contractor* means 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 Education Law §211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

(t) *Unauthorized Disclosure or Unauthorized Release* means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

§121.2 Educational Agency Data Collection Transparency and Restrictions.

(a) Educational agencies shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(b) Each educational agency shall take steps to minimize its collection, processing and transmission of personally identifiable information.

(c) Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with federal and state law and the educational agency's data security and privacy policy.

(d) 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.

§121.3 Bill of Rights for Data Privacy and Security.

(a) Each educational agency shall publish on its website a parents bill of rights for data privacy and security ("bill of rights") that complies with the provisions of Education Law §2-d (3).

(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information.

(c) The bill of rights shall also include supplemental information for each contract the educational agency enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data. The supplemental information must be developed by the educational agency and include the following information:

(1) the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

(2) how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);

(3) the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).

(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;

(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 and data security and privacy risks mitigated; and

(6) address how the data will be protected using encryption while in motion and at rest.

(d) Each educational agency shall publish on its website the supplement to the bill of rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable information.

(e) The bill of rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the educational agency's data and/or technology infrastructure.

§121.4 Complaints of Breach or Unauthorized Release of Personally Identifiable Information

(a) Each educational agency must establish and communicate to parents, eligible students, teachers, principals or other staff of an educational agency, its procedures for them to file complaints about breaches or unauthorized releases of student data and/or teacher or principal data.

(b) The complaint procedures must require educational agencies to promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information.

(c) Following its investigation of a submitted complaint, the educational agency shall provide the parent or eligible student, teacher, principal or any other staff member of the educational agency who filed a complaint with its findings within a reasonable period but no more than 60 calendar days from the receipt of the complaint by the educational agency. Where the educational agency requires additional time, or where the response may compromise security or impede a law enforcement investigation, the educational agency shall provide the parent, eligible student, teacher, principal or any other staff member of the educational agency who filed a complaint with a written explanation that includes the approximate date when the educational agency anticipates that it will respond to the complaint.

(d) Educational agencies may require complaints to be submitted in writing.

(e) Educational agencies must maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

§121.5 Data Security and Privacy Standard.

(a) As required by Education Law §2-d (5), the Department adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the standard for data security and privacy for educational agencies.

(b) No later than July 1, 2020, each educational agency shall adopt and publish a data security and privacy policy that implements the requirements of this Part and aligns with the NIST CSF.

(c) Each educational agency's data security and privacy policy must also address the data privacy protections set forth in Education Law §2-d (5)(b)(1) and (2) as follows:

(1) every use and disclosure of personally identifiable information by the educational agency shall benefit students and the educational agency (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

(2) personally identifiable information shall not be included in public reports or other documents.

(d) An educational agency's data security and privacy policy shall include all the protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes.

(e) Each educational agency must publish its data security and privacy policy on its website and provide notice of the policy to all its officers and employees.

§121.6 Data Security and Privacy Plan.

(a) Each educational agency that enters into a contract with a third-party contractor shall ensure that the contract includes the third-party contractor's data security and privacy plan that is accepted by the educational agency. The data security and privacy plan shall, at a minimum:

(1) outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;

(2) specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;

(3) demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

(4) specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

(5) specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

(6) specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

(7) describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

§121.7 Training for Educational Agency Employees.

Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include but not be limited to training on the state and federal laws that protect personally identifiable information, and how employees can comply with such laws. Such training may be delivered using online training tools and may be included as part of training the educational agency already offers to its workforce.

§121.8 Educational Agency Data Protection Officer

(a) Each educational agency shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency.

(b) Data Protection Officers must have the appropriate knowledge, training and experience to administer the functions described in this Part.

(c) A current employee of an educational agency may perform this function in addition to other job responsibilities.

§121.9 Third Party Contractors

(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:

(1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;

(2) comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part;

(3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

(4) not use the personally identifiable information for any purpose not explicitly authorized in its contract;

(5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student:

(i) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

(ii) unless required by statute or court order and the third-party contractor provides a notice of 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 disclosure is expressly prohibited by the statute or court order.

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

(7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and

(8) not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(b) Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

§121.10 Reports and Notifications of Breach and Unauthorized Release

(a) Third-party contractors shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.

(b) Each educational agency shall in turn notify the Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the Department.

(c) Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

(d) Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

(e) Educational agencies shall notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release by an educational agency or the receipt of a notification of a breach or unauthorized release from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of personally identifiable information by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the educational agency shall notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

(f) Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor shall pay for or promptly reimburse the educational agency for the full cost of such notification.

(g) Notifications required by this section shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.

(h) Notification must be directly provided to the affected parent, eligible student, teacher or principal by first-class mail to their last known address; by email; or by telephone.

(i) Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer shall report such breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

§121.11 Third Party Contractor Civil Penalties

(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. Each violation of this paragraph by a third-party contractor shall be punishable by a civil penalty of the greater of $5,000 or up to $10 per student, teacher, and principal whose data was released, provided that the latter amount shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a).

(b) Except as otherwise provided in subdivision (a) each violation of Education Law §2-d by a third-party contractor or its assignee shall be punishable by a civil penalty of up to $1,000.00; a second violation by the same third party contractor involving the same data shall be punishable by a civil penalty of up to $5,000; any

subsequent violation by the same third party contractor involving the same data shall be punishable by a civil penalty of up to $10,000. Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law §899-aa (6) (a).

(c) The Chief Privacy Officer shall investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine and/or inspect the third-party contractor's facilities and records.

(d) Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive such data in violation of applicable state or federal law, the data and security policies of the educational agency, and/or any binding contractual obligations, the Chief Privacy Officer shall notify the third-party contractor of such finding and give the third-party contractor no more than 30 days to submit a written response.

(e) () If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law §2-d, the Chief Privacy Officer shall be authorized to:

(1) order the third-party contractor be precluded from accessing personally identifiable information from the affected educational agency 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 breach or 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 who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data shall not be deemed a responsible bidder or offeror 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 General Municipal Law §103 or State Finance Law §163(10)(c), as applicable, for a fixed period of up to five years;

(4) require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to such data and certify that it has been performed, at the contractor's expense. Such additional training must be performed immediately and include a review of federal and state laws, rules, regulations, including Education Law §2-d and this Part.

(f) If the Chief Privacy Officer determines that the breach or 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 Chief Privacy Officer would make a recommendation to the Commissioner that no penalty be issued upon the third-party contractor. The Commissioner would then make a final determination as to whether the breach or 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 and whether or not a penalty should be issued.

§121.12 Right of Parents and Eligible Students to Inspect and Review Students Education Records

(a) Consistent with the obligations of the educational agency under FERPA, parents and eligible students shall have the right to inspect and review a student's education record by making a request directly to the educational agency in a manner prescribed by the educational agency.

(b) An educational agency shall ensure that only authorized individuals are able to inspect and review student data. To that end, educational agencies shall take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

(c) Requests by a parent or eligible student for access to a student's education records must be directed to an educational agency and not to a third-party contractor. An educational agency may require that requests to inspect and review education records be made in writing.

(d) Educational agencies are required to notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by an educational agency. A notice issued by an educational agency to comply with the FERPA annual notice requirement shall be deemed to satisfy this requirement. Two separate annual notices shall not be required.

(e) Educational agencies shall comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

(f) Educational agencies may provide the records to a parent or eligible student electronically, if the parent consents to such a delivery method. The educational agency must transmit the personally identifiable information in a way that complies with State and federal law and regulations. Safeguards associated with industry standards and best practices, including but not limited to, encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

§121.13 Chief Privacy Officer's Powers

(a) The Chief Privacy Officer shall have the power to 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, which shall include but not be limited to records related to any technology product or service that will be utilized to store and/or process personally identifiable information.

(b) Based upon a review of such records, the Chief Privacy Officer may require an educational agency to act to ensure that personally identifiable information is protected in accordance with state and federal law and regulations, including but not limited to requiring an educational agency to perform a privacy impact and security risk assessment.

(c) The Chief Privacy Officer shall also have and exercise any other powers that the commissioner shall deem appropriate.

§ 121.14 Severability.

If any provision of this Part or its application to any person or circumstances is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or their application to other persons and circumstances, and those remaining provisions shall not be affected but shall remain in full force and effect.