PARENT COALITION FOR STUDENT PRIVACY

www.studentprivacymatters.org
info@studentprivacymatters.org
@parents4privacy

124 Waverly Place
New York, NY 10011
303.204.1272

NYS Student Privacy Regulations For NY Education Law § 2d

Important Regulatory Definitions (8 CRR-NY 121.1)

Commercial or Marketing Purpose – Selling, using, or disclosing student data for payment or advertising, or developing, improving, or marketing products or services to students.

Disclose or Disclosure – Intentionally or unintentionally releasing, transferring, communicating, or permitting access to PII.

Educational Agency – The NY State Education Department, schools, School districts, and BOCES.

Education Records – Materials containing info directly related to students which are maintained by an educational agency or a person acting for an agency (20 USC § 1232g(a)(4)).

Encryption – Using technology to render PII unusable or unreadable to unauthorized people.

Personally Identifiable Information (PII) – Names and addresses of students or their families, personal identifiers of students (e.g., social security number, birthday, birthplace, and mother's maiden name), and info enabling a school community member to ID a student (34 CFR § 99.3).

Student – Any person attending or seeking to enroll in an educational agency.

School – Public elementary or secondary schools, including charter schools, publicly funded pre-k programs and programs in NYC's universal pre-k, approved preschool special education providers and schools for students with disabilities, schools in special act school districts.

Student Data – PII from an educational agency's student records.

Third-Party Contractor – People and entities, other than educational agencies, receiving student data from an educational agency based on a contract or written agreement to provide services (e.g., store or manage data, conduct studies, or evaluate publicly funded programs).

Data Collection Transparency and Restrictions (8 CRR-NY 121.2)

Educational agencies cannot sell, use, or disclose PII for marketing or commercial purposes, or facilitate its use or disclosure by others for marketing or commercial purposes. Educational agencies shall include provisions in contracts with third-parties or in separate data sharing and confidentiality agreements requiring confidentiality of shared student data. Educational agencies shall take steps to minimize collection, processing and transmission of PII. 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:

- juvenile delinquency records;
- criminal records;
- medical and health records; and
- student biometric information.

Data Privacy and Security Bill of Rights (8 CRR-NY 121.3)

Each educational agency shall publish a parents bill of rights for data privacy and security.

The bill of rights shall be included with every contract an educational agency enters with a third-party contractor that receives PII.

The bill of rights shall 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:

- the exclusive purposes for which the third-party contractor will use the student data;
- 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, if any, will abide by applicable data protection and security requirements;
- the contract's duration, including its expiration date and a description of what will happen to student data when the contract or written agreement's expires (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).
- how a parent, eligible student, teacher or principal can access the data in order to challenge the accuracy of the data that is collected;
- where student 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
- address how the data will be protected using encryption while in motion and at rest.

Educational agencies shall publish the supplement to the bill of rights for any contract or other written agreement with a third-party contractor that will receive personally identifiable info.

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

Complaints of Breach or Unauthorized Release of PII (8 CRR-NY 121.4)

Educational agencies must establish and communicate to parents, eligible students, teachers, principals or other staff, its procedures to file complaints about breaches or unauthorized releases of student data and/or teacher or principal data. Complaint procedures must require educational agencies to promptly acknowledge receipt of complaints, commence an investigation, and take necessary precautions to protect PII.

Following its investigation complaint, the educational agency shall provide the person who filed a complaint with its findings within a reasonable period but no more than 60 calendar days from the receipt of the complaint. 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 complainant with a written explanation that includes the approximate date when the educational agency anticipates that it will respond to the complaint. Educational agencies may require complaints to be submitted in writing.

Data Security and Privacy Standard (8 CRR-NY 121.5)

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

- Every use and disclosure of PII 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).
- PII cannot be included in public reports or other documents.

Data Security and Privacy Plan (8 CRR-NY 121.6)

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:

- 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;
- specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that it will receive under the contract;
- demonstrate that it complies with the requirements of section 121.3(c) of this Part;
- specify how officers or employees of the third-party contractor and its assignees who have access to student data receive or will receive training on the Federal and State laws governing confidentiality of such data prior to receiving access;
- specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable info is protected;
- 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;
- 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 ends.

Training for Educational Agency Employees (8 CRR-NY 121.7)

Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to PII. Training should include but not be limited to training on the State and Federal laws that protect PII, 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.

Educational Agency Data Protection Officer (8 CRR-NY 121.8)

Each educational agency shall designate a data protection officer to be responsible for the implementation of the policies and procedures required in Education Law section 2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency. Data protection officers must have the appropriate knowledge, training and experience to administer the functions described in these regulations. A current employee of an educational agency may perform this function in addition to other job responsibilities.

Third-Party Contractors (8 CRR-NY 121.9)

Third-party contractors (and their subcontractors) that will receive student data must:

- adopt technologies and practices aligned with the NIST Cybersecurity Framework;
- comply with the data security and privacy policy of the agency with whom it contracts; Education Law section 2-d; and this Part;
- limit internal access to PII to only those employees or subcontractors that need access to provide the contracted services;
- not use the PII for any purpose not explicitly authorized in its contract or disclose PII to another party without prior written consent of the parent or eligible student:
    - 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
    - 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 info no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order;
- maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
- use encryption to protect PII in its custody while in motion or at rest; and
- not sell, disclose, or use PII for marketing or commercial purposes or facilitate its use or disclosure by another party for marketing or commercial purposes or permit another party to do so.

Reports And Notifications Of Breach And Unauthorized Release (8 CRR-NY 121.10)

Third-party contractors shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of PII in the most expedient way possible and without unreasonable delay but no more than 7 calendar days after discovering such breach.

Each agency must 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.

Third-party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Agencies shall report every discovery or report of a breach or unauthorized release of student data to the chief privacy officer without unreasonable delay, but no more than 10 calendar days after such discovery.

Educational agencies must notify parents and eligible students as expediently as possible and without unreasonable delay, but no more than 60 calendar days after discovering a breach or unauthorized release by an agency or receipt of a notification of a breach or unauthorized release from a third-party contractor unless notification interferes with an ongoing investigation by law enforcement or causes further disclosure of PII by disclosing an unfixed security vulnerability. If such circumstances delay notification, the agency must 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.

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

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 PII 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.

Notification must be directly provided to affected parents or eligible students by email, phone, or first-class mail to a last known address. 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 as expediently as possible, without unreasonable delay.

Third-party Contractor Civil Penalties (8 CRR-NY 121.11)

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 section 899-aa(6)(a)***.

Right Of Parents And Eligible Students To Inspect And Review Students Education Records (8 CRR-NY 121.12)

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.

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.

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.

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. 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.

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.

Chief Privacy Officer's Powers (8 CRR-NY 121.13)

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. 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. The chief privacy officer shall also have and exercise any other powers that the commissioner shall deem appropriate.

Severability (8 CRR-NY 121.14)

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.