Parent FAQ

Frequently Asked Questions About Data Privacy and Security

1. Can companies that provide services to my school under contract (third party contractors) buy my information or use it for their marketing purposes?
No. Your personally identifiable information (PII) cannot be sold by a contractor or used for marketing purposes.

2. Must I be notified if there is an unauthorized disclosure of my personally identifiable information?
Yes. The school must notify the parent or eligible student of the unauthorized release of student data in the most expedient way possible and without unreasonable delay. This applies to cases of an unauthorized release of teacher or principal personally identifiable information data as well. Each affected teacher or principal must be notified.

3. What other laws protect my student's data?
In addition to New York's Education Law Section 2-d, there are federal laws that are designed to protect student data and prohibit any misuse. The Family Educational Rights and Privacy Act (FERPA) is the foundational federal law on the privacy of students' educational records. It was enacted in 1974 and applies to schools that receive federal funding, which are most public schools and some, but not all, private schools. FERPA safeguards student privacy by limiting who may access student records, specifying for what purpose they may access those records, and detailing what rules they have to follow when accessing the data. FERPA also includes provisions that guarantee a parent's right to access, review and request the correction of their child's educational record. For additional information about FERPA and other federal laws, please visit our page, Federal Laws that Protect Student Data. Other applicable laws are the Protection of Pupil Rights Amendment (PPRA) which defines the rules states and school districts must follow when administering tools like surveys, analysis, and evaluations funded by the US Department of Education to students, and the Children's Online Privacy Protection Rule (COPPA) which imposes certain requirements on operators of websites, games, mobile apps or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

4. How will contracted service providers be held accountable for maintaining the confidentiality of the student data they receive?
Educational agencies that contract with third parties who will receive student PII must enter into contracts with such third parties which include certain conditions outlined in the law such as the inclusion of a data security and privacy plan, the parents bill of rights and minimum technical security standards to protect student PII. The Chief Privacy Officer is also authorized by the law to impose civil penalties.

5. What are the essential parents' rights under the Family Educational Rights and Privacy Act (FERPA) relating to personally identifiable information in their child's student records?

The rights of parents under FERPA are summarized in the Model Notification of Rights prepared by the United States Department of Education for use by schools in providing annual notification of rights to parents.

Parents' rights under FERPA include:

1.
   - The right to inspect and review the student's education records within 45 days after the day the school or school district receives a request for access.
   - The right to request amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Complete student records are maintained by schools and school districts and not at NYSED, therefore, NYSED cannot make amendments to school or school district records. Schools and school districts are best positioned to make corrections to students' education records.
   - The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to: (i) school officials within the school or school district with legitimate educational interests; (ii) officials of another school for purposes of enrollment or transfer; (iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED; (v) organizations conducting studies for or on behalf of educational agencies) and (vi) the public where the school or school district has designated certain student data as "directory information" (described below). The FERPA Model Notification of Rights more fully describes the exceptions to the consent requirement under FERPA).
   - Where a school or school district has a policy of releasing "directory information" from student records, the parent has a right to refuse to let the school or school district designate any of such information as directory information. Directory information, as defined in federal regulations, includes: the student's name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, enrollment status, dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received and the most recent educational agency or institution attended. Where disclosure without consent is otherwise authorized under FERPA, however, a parent's refusal to permit disclosure of directory information does not prevent disclosure pursuant to such separate authorization.
   - The right to file a complaint with the U.S. Department of Education concerning alleged failures by the School to comply with the requirements of FERPA.

6. What "educational agencies" are included in the requirements of Education Law §2-d?

•

- The New York State Education Department ("NYSED");
- Each public school district;
- Each Board of Cooperative Educational Services or BOCES; and
- All schools that are:
  - a public elementary or secondary school;
  - universal pre-kindergarten program authorized pursuant to Education Law §3602-e;
  - an approved provider of preschool special education services; o any other publicly funded pre-kindergarten program;
  - a school serving children in a special act school district as defined in Education Law 4001; or
  - certain schools for the education of students with disabilities – an approved private school, a state-supported school subject to the provisions of Education Law Article 85, or a state-operated school subject to Education Law Article 87 or 88.

7. What kind of student data is subject to the confidentiality and security requirements of Education Law §2-d?

The law applies to personally identifiable information contained in student records of an educational agency listed above. The term "student" refers to any person attending or seeking to enroll in an educational agency, and the term "personally identifiable information" ("PII") uses the definition provided in FERPA. Under FERPA, personally identifiable information or PII includes, but is not limited to:

1.
   - The student's name;
   - The name of the student's parent or other family members;
   - The address of the student or student's family;
   - A personal identifier, such as the student's social security number, student number, or biometric record;
   - Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name;
   - 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; or
   - Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

8.What kind of student data is *not* subject to the confidentiality and security requirements of Education Law §2-d?

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de-identified data (e.g., data regarding students that uses random identifiers), aggregated

data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student is not considered to be PII and is not within the purview of Education Law §2-d.

9. What protections are required to be in place if an educational agency contracts with a third-party contractor to provide services, and the contract requires the disclosure of PII to the third party contractor?

Education Law §2-d provides very specific protections for contracts with "third party contractors", defined as 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. The term "third party contractor" also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an "educational agency."

Services of a third-party contractor covered under Education Law §2-d include, but not limited to, data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs.

When an educational agency enters into a contract with a third-party contractor, under which the third-party contractor will receive student data, the contract or agreement must include 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. However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents' Bill of Rights must be included, as well as 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.

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 must also comply with additional requirements outlined in Education Law §2-d such as limiting internal access to education records to those individuals that are determined to have legitimate educational interests, not using the education records for any other purposes than those explicitly authorized in its contract; not disclosing any PII to any other party that is not an authorized representative of the third party contractor to the extent they are carrying out the contract (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 NYSED, 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; maintaining reasonable administrative, technical and

physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and using encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

10. What steps can and must be taken in the event of a breach of confidentiality or security?

NYSED's Chief Privacy Officer is 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 APPR data. Where there is a breach and unauthorized release of PII by a third-party contractor or its assignees, the third-party contractor must notify NYSED of the breach in the most expedient way possible and without unreasonable delay. NYSED must then notify the parents in the most expedient way possible and without unreasonable delay. The law also authorizes the Chief Privacy Officer to impose certain penalties such as a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.