

New York Education Law Section 2D: Student Data Privacy and Regulations

New York [State Ed Law § 2D](#) and its legally enforceable [regulations](#) restrict how districts, schools and their contractors may collect, use and share personal student data

- NYSED, districts and their contractors/vendors cannot sell, use or disclose student personally identifiable info (PII) for marketing or commercial purposes or allow its sale or disclosure by others for these purposes.
- School districts cannot report medical, criminal, or juvenile delinquency records to NYSED except as required by law.
- Districts must minimize collection & transmission of PII and its use and disclosure must benefit students (e.g., improve academic achievement, empower parents and students, and/or advance effective school operations)
- NYSED, districts and their contractors/vendors must provide parents and eligible students with the means to inspect their education records by request, and comply with such requests within 45 days.

There are also requirements for districts and vendors regarding the storage and security of student data

- NYSED & districts must require third-party contractors receiving any personal student data to:
 - maintain student data confidentiality
 - adopt federally, state, and agency-compliant data security protection policies and practices, and encrypt PII in motion and at rest, in alignment with NIST Cybersecurity Version 1.1
 - limit access to PII to only those who need access to provide contracted services, or receive consent from parents or eligible students beforehand
 - notify districts of PII breaches or unauthorized access within 7 calendar days of discovering a breach
- NYSED and/or districts must establish process for parental complaints for unauthorized disclosure of their children's PII & parents should receive a response of following investigations in no more than 60 calendar days
- NYSED & districts must notify parents and eligible students of any data breaches or unauthorized access within 60 calendar days of their discovery
- NYSED & districts must adopt and publish on websites their Data Security and Privacy Policies by October 1, 2020

A Parent Bill of Rights must be included in every contract and must be published online

- A Parent Bill of Rights for data privacy and security must be included in every NYSED, district or school contract or agreement with third-parties with access to student PII
- This Bill of Rights shall include the following supplemental information, which must be published on the NYSED, district or school website for each of their contracts or agreements
 - what the third party will use the student data for
 - how parents can access the data for their children to be able to challenge its accuracy
 - where the data will be stored and what security will be used to protect it, including how data will be encrypted in motion and at rest
 - how any subcontractors will comply with the same privacy & security provisions
 - describe the plan for notification to parents and remediation if there are unauthorized disclosures
 - explain how long the contract will last and describe if, how, and when data will be returned to the district, transitioned to a successor contractor, and/or destroyed when the contract is terminated or ends

Mandate for Data Protection officers and annual staff training

- NYSED & districts must provide annual training in data privacy & security to all employees & officers with access to PII & districts must designate Data Protection Officers responsible for ensuring legal compliance

For a more detailed summary see [here](#). For more information, contact the Parent Coalition for Student Privacy at info@studentprivacymatters.org or NYSAPE at nys.allies@gmail.com