BILL OF RIGHTS

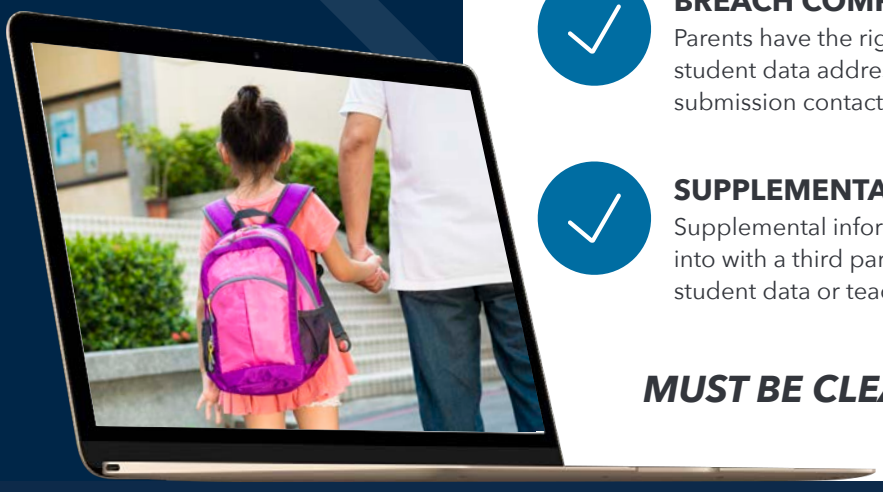
A Parents' Bill of Rights for Data Privacy and Security must be published on the website of each educational agency and must be included with every contract an educational agency enters into with a third-party contractor that receives personally identifiable information. The list below highlights required elements that must be included in the Parents' Bill of Rights. To learn more about this requirement, agencies can review Part 121.3 of the Regulations and Section 3 of Education Law 2-d.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Bill of Rights:

- ✓ Includes All Elements
- ✓ Is Posted on the District's Website
- ✓ Includes Supplemental Information for All Relevant Contracts
- ✓ Is Included and Signed in All Relevant Contracts



REQUIRED ELEMENTS

DATA WILL NOT BE SOLD
A student's personally identifiable information cannot be sold or released for any commercial purposes

THE RIGHT TO REVIEW CHILD'S RECORD
Parents have the right to inspect and review the complete contents of their child's education record

DATA IS PROTECTED
State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices must be in place when data is stored or transferred

NYSED COLLECTED DATA
A complete list of all student data elements collected by the State is available for public review. Districts must include an appropriate NYSED link and NYSED mailing address for parents.

BREACH COMPLAINT CONTACT
Parents have the right to have complaints about possible breaches of student data addressed. Districts must include appropriate complaint submission contact information (e.g. phone number, email and address).

SUPPLEMENTAL INFORMATION
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.

MUST BE CLEAR AND IN PLAIN ENGLISH

BILL OF RIGHTS SUPPLEMENTAL INFORMATION

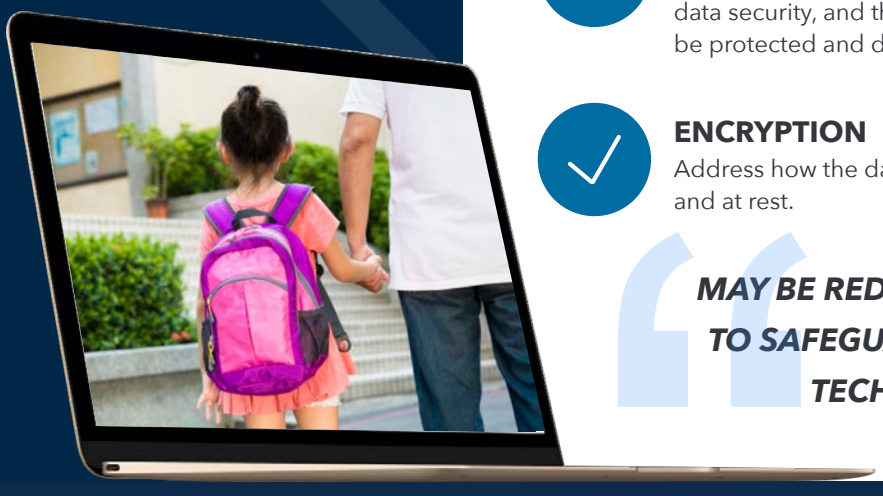
Educational agencies are required to post information about third-party contracts on the agency's website with the Bill of Rights. Supplemental information may be redacted to the extent necessary to safeguard the data. To learn more about this requirement, review Part 121.3 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Supplmental Information:

- ✓ Includes All Elements
- ✓ Is Posted on the District's Website
- ✓ Includes Supplemental Information for All Relevant Contracts
- ✓ Includes Links or Attachments to Relevant BOCES/RIC Contracts



REQUIRED ELEMENTS

The supplemental information must be developed by the educational agency and include the following information:

EXCLUSIVE PURPOSE FOR DATA USE
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;

SUBCONTRACTORS MANAGEMENT
How the contractor will ensure that the subcontractors, if any, will abide by all applicable data protection requirements, including but not limited to those outlined in applicable state and federal laws and regulations;

CONTRACT DURATION AND DATA DESTRUCTION
The duration of the contract, including the contract's expiration date and a description of what will happen to the data upon expiration of the contract or other written agreement;

DATA ACCURACY
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;

LOCATION OF THE DATA AND SECURITY PRACTICES
Where the 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;

ENCRYPTION
Address how the data will be protected using encryption while in motion and at rest.

MAY BE REDACTED TO THE EXTENT NECESSARY TO SAFEGUARD THE AGENCY'S DATA AND/OR TECHNOLOGY INFRASTRUCTURE

MODEL PARENTS' BILL OF RIGHTS

DISTRICT seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our operations. To assist in meeting legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law, DISTRICT has posted this Parents Bill of Rights for Data Privacy and Security.

(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. The procedures for exercising this right can be found in Student Records Policy, No. [Insert Number].

(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 at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed.

- Parents may make a written report of a possible breach of student data to the DISTRICT Data Protection Officer by email at [Insert e-mail address] or by regular mail at [insert address].
- Complaints may also be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 1223 or by submitting a form at: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

We are compiling the following information about each agreement between DISTRICT and an outside party that receives protected student data, or protected principal or teacher data, from the district: (1) the exclusive purposes for which the data will be used, (2) how the contractor will ensure that any subcontractors it uses will abide by data protection and security requirements, (3) when the contract expires and what happens to the data at that time, (4) if and how an affected party can challenge the accuracy of the data, (5) where the data will be stored, and (6) the security protections taken to ensure the data will be protected, including whether the data will be encrypted. The links below will take you to that information for the listed agreements. We will be updating this list as we gather additional information.

MODEL SUPPLEMENTAL INFORMATION

The supplemental information must reflect the language of each specific data sharing agreement with a vendor. An example is provided below.

CONTRACTOR	[Vendor Name]
PRODUCT	[Product Name]
PURPOSE DETAILS	The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT. The product or services are used to provide [e.g., mathematics instruction in Grades 1 and 2].
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.
CONTRACT DURATION AND DATA DESTRUCTION INFORMATION	The agreement expires [Insert Date]. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT. Upon expiration of this Contract with a successor agreement in place, Vendor will cooperate with the DISTRICT as necessary to transition protected data to the successor vendor prior to deletion. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
DATA ACCURACY INFORMATION	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Education Rights and Privacy Act.
SECURITY PRACTICES INFORMATION	The data is stored in the continental United States (CONUS) or Canada. Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0. Vendor will use 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 U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).