

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Vendor is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the District and Vendor to the contrary, Vendor agrees as follows:

Vendor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Vendor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Vendor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Vendor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Vendor shall have in place sufficient internal controls to ensure that the District Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

Personally identifiable information from the records of the District 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

Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Vendor agrees to comply with District policy(ies) on data security and privacy.

Vendor shall promptly reimburse District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Vendor shall return all of the District's data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of the District's Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Vendor's possession and use of Protected Data pursuant to this Agreement.
2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Vendor's policy on data security and privacy.
3. An outline of the measures taken by Vendor to secure Protected Data and to limit access to such data to authorized staff.
4. An outline of how Vendor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.
5. An outline of how Vendor will ensure that any subcontractors, persons or entities with which Vendor will share Protected Data, if any, will abide by the requirements of Vendor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA PRIVACY AND SECURITY PLAN

Edmentum's document include our Customer Privacy Policy, COPPA and FERPA Assurance Statement, and the Student Privacy Pledge, which is already extremely thorough and should address any concerns. These documents are public and reside on our website.

1. Edmentum's Standard Terms - <http://www.edmentum.com/standardterms>
2. Customer Privacy Policy - <http://www.edmentum.com/Privacy>
3. Edmentum's Assurance to COPPA - <http://www.edmentum.com/coppa>
4. Edmentum's Assurance to FERPA - <http://www.edmentum.com/ferpa>
5. Student Privacy Pledge - <http://www.studentprivacypledge.org>

Edmentum, Inc.



Jamie Candee, President/CEO