## EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1.  A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2.  The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3.  State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4.  Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5.  A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security, and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6.  The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7.  To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8.  Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9.  Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

# Attachment to Contractor's[1]
# Data Security and Privacy Plan

1. Specify whether this Contract involves disclosure to the Contractor of Student Data, APPR Data, or both.

    X Disclosure of Student Data

    X Disclosure of APPR Data

2. Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

    > The data will be used to meet state and federal reporting and accountability requirements.

3. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR in the performance of this Contract, and describe how the Contractor will ensure that such persons/entities will abide by the data protection and security requirements of the Contract.

    Subcontractors or other entities with whom the Contractor will share  data:

    > CDN Associates Inc., AduroTech Inc, Sentient Software Solutions Inc., ThomSand Consulting Services, GST BOCES and Eastern Suffolk BOCES. Each of these entities agree in writing to abide by the applicable provisions of Contractor's Data Security and Privacy Plan.

    ***In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or another entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Contract including, but not limited to, the "Data Security and Privacy Plan." Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to Contractor or otherwise destroyed as provided in Paragraph 4 of the "Data Security and Privacy Plan."***

4. Specify the expiration date of the Contract, and explain what will happen to the Student Data or APPR Data in the Contractor's possession, or the possession of any person/entity described in response to Paragraph 3, upon the expiration or earlier termination of the Contract.

    Contract expiration date: <u>7/31/2025</u>

    <u>X</u> Contractor agrees to return the Student or APPR Data to NYSED consistent with the protocols set forth in the "Data Security and Privacy Plan."

---

[1] The term "Contractor" herein refers to Erie 1 BOCES, which is an educational agency under NYS Education Law §2-d, on behalf of the Western New York Regional Information Center.

__ Contractor agree to securely destroy the Student Data or APPR Data consistent with the protocols set forth in the "Data Security and Privacy Plan."

5.  State whether the Contractor will be collecting any data from or pertaining to students derived from the student's education record, or pertaining to teachers or principals' annual professional performance evaluation pursuant to the Contract, and explain if and how a parent, student, eligible student (a student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR data that is collected.

>   X Student Data
>
>   X APPR Data
>
>   ***Any challenges to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated or otherwise created such data.***

6.  Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize data security), and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

> The student data or APPR data will be stored on dedicated servers with appropriate VPN tunnels with approved security protections ensuring data is encrypted in transit and at rest. Contractor will utilize an advanced encryption standard (AES).