

EXHIBIT 2 - Education Law § 2-d Bill of Rights for Data Privacy and Security and
Supplemental Information for Contracts that Utilize Personally Identifiable Information

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 ("Student PII") cannot be sold or released for any Commercial or Marketing purpose. Student 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 Regulations of the Commissioner of Education 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 Student PII.
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 New York State Education Department ("NYSED") is available at www.nysed.gov/data-privacy-security/student-data-inventory 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 Student PII addressed. Complaints should be submitted to the NYS Education Department at 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 Student PII is either unlawfully accessed or unlawfully disclosed.
8. NYSED workers that have access to or receive disclosure of Student PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. NYSED contracts with vendors that receive Student PII will address statutory and regulatory data privacy and security requirements.

Supplemental Information

Pursuant to Education Law § 2-d and § 121.3 of the Regulations of the Commissioner of Education, NYSED is required to post information to its website about its contracts with third-party contractors that will be provided Access to or receive Disclosure of Student Data and/or APPR Data.

1. Name of Contractor:

Queens College, City University of New York, on behalf of the Research Institute for the Study of Language in Urban Society (RISLUS)

2. Description of the exclusive purpose(s) for which the Student Data and/or APPR Data will be used:

Using Student Data effectively and responsibly is foundational to making informed student educational decisions. Capturing accurate information is necessary for state reporting to NYSED regarding newcomer and SIFE assessment in New York State. State and federal laws establish baseline parameters for what is permissible when collecting and sharing student information. We use additional applicable state and federal guidelines and strict processes to protect the privacy of every student and to ensure the confidentiality and security of all data we collect.

3. Type(s) of Data that Contractor will be provided Access to or Disclosure of:

Student Data Yes No

APPR Data Yes No

4. Contract Term:

Contract Start Date: July 1, 2023

Contract End Date: June 30, 2028

5. Subcontractor use and written agreement requirement:

Contractor will use Subcontractors Yes No

Contractor will not use Subcontractors Yes No

If Contractor plans to use Subcontractors, Contractor will not utilize Subcontractors without a written contract that requires the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Contractor by state and federal laws and regulations and this contract.

Contractor agrees to bind its Subcontractors by written agreement. Yes No

Not Applicable because Contractor will not use Subcontractors. N/A Yes No

6. Data Transition and Secure Destruction

Yes No Contractor agrees that the confidentiality and data security obligations under this DPA will survive the expiration or termination of this contract but shall terminate upon Contractor’s certifying, that Contractor and its Subcontractors:

- Are unable to Access any Information provided to Contractor pursuant to this contract
 - Securely transfer Disclosed Student Data and APPR Data to NYSED, or at NYSED’s option and written discretion, a successor contractor in a format agreed to by the Parties.
 - Securely delete and destroy Disclosed Student Data and APPR Data.

7. Challenges to Data Accuracy

Yes No Contractor agrees that parents, eligible students, teachers, or principals who seek to challenge the accuracy of Student Data or APPR Data will be referred to NYSED and if a correction to data is deemed necessary, NYSED will notify Contractor. Contractor further agrees to facilitate such corrections within 21 days of receiving NYSED’s written request.

8. Secure Storage and Data Security

Please indicate where Student Data and/or APPR Data will be stored:

Yes No Using a cloud or infrastructure owned and hosted by a third party.

Yes **No** Using Contractor owned and hosted solution

Yes **No** Other:

Please describe how data privacy and security risks will be mitigated in a manner that does not compromise the security of the data:

All applicable data privacy and security contract requirements will be implemented over the life of the contract, including compliance with the law; using Student Data only to provide authorized services; ensuring only authorized personnel access Student Data and that all authorized personnel have appropriate training; and regularly auditing our systems to ensure compliance.

All data in the database is encrypted. If unauthorized access occurs, data will not be readable. All data security protocols comply with New York law and regulations to preserve and protect Information. Information at rest and in transit is encrypted in accordance with applicable New York laws and regulations. In case of a Breach, NYSED will be notified within 7 days of discovery of a Breach in accordance with NYSED regulations.

9. Encryption requirement

Contractor agrees that Student Data and APPR Data will be encrypted while in motion and at rest.

Yes No

10. Contractor Certification.

Contractor certifies that Contractor will comply with, and require its Subcontractors to comply with, applicable State and Federal laws, rules, and regulations and NYSED policies.

Contractor’s Name: Queens College, City University of New York, on behalf of the Research Institute for the

Study of Language in Urban Society (RISLUS)

Signature

Printed Name

Title

Date