NON DISCLOSURE / DATA PROCESSING AGREEMENT
FOR SERVICES AND FUNCTIONS PROVIDED ON BEHALF OF THE BOE

This agreement ("Agreement") is dated [Insert Date] between
The Board of Education of the City of New York with an address at 52 Chambers Street, New York, New York 10007 ("BOE", "DOE" or "NYC DOE")
and
[Insert Company Name] ("Processor") with an address at [Insert Address]

The Processor agrees as follows:

1. Definitions.

"BOE Technology Assets" means all BOE facilities, BOE systems, BOE telecommunications, electronic data created, processed, accessed, transferred, stored, or disposed of by BOE systems, and such systems' peripheral equipment, networks, or magnetic data, and any electronic data created, processed, accessed, transferred, stored, or disposed of by such systems.

"Cloud Service/s" means the software-, platform-, infrastructure- or other "as a service" solution for which access is provided by Processor to the BOE under this Agreement, including any client software provided to the BOE by Processor for use with the Cloud Service. Any software to be installed on the BOE's hardware for the purpose of facilitating the BOE's use of the Cloud Services shall be deemed to be a part of the Cloud Services.

"Confidential Information" means (a) Protected Information; (b) any personally identifiable information related to BOE employees, agents and/or volunteers obtained by or furnished to the Processor; (c) all findings, analysis, data, reports or other information, whether in oral, written, graphic, or machine-readable form, obtained from the BOE or furnished by the BOE to the Processor in connection with the Services; and (d) all information marked "confidential" in writing.

Confidential Information excludes any information that both (a) is not Protected Information and (b) is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of the Processor in breach of this Agreement, (ii) demonstrated to have been known to the Processor prior to disclosure by or through the BOE, (iii) disclosed with the prior written approval of the BOE, (iv) demonstrated to have been independently developed by the Processor without reference to the Confidential Information, and (v) disclosed to the Processor by a third party under conditions permitting such disclosure, without breach of this Agreement.

"NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, or any successor thereto.

"Process" or "Processing" means to perform any act, omission or operation on or with respect to data or information, such as accessing, adapting, altering, blocking, collecting, combining, delivering, deleting, destroying, disclosing, disseminating, erasing, generating, learning of, organizing, recording, releasing, retrieving, reviewing, sharing, storing, transmitting, using or otherwise making data or information available.

"Processor Systems" means the facilities, systems, networks and IT environments that are used to Process any Confidential Information, deliver any Cloud Services or to otherwise meet any of Processor's obligations under this Agreement.

"Protected Information," as it relates to (a) BOE's current, future and former students and their families, consists of "personally identifiable information" as defined by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA;") and (b) as it relates to certain BOE employees, consists of "personally identifying information" as that term is used in New York Education Law 3012-c(10). In the case of either (a) or (b), Protected Information shall consist of any such information

Processed by the Processor in the course of providing the Services, whether disclosed or provided by the BOE or collected, accessed or generated by the Processor in some other manner.

"Security Incident" means an event that compromises or is suspected to compromise the security, confidentiality, availability or integrity of Confidential Information, BOE Technology Assets or Processor Systems, including by compromising the physical, technical, administrative or organizational safeguards implemented by Provider to protect the security, confidentiality, availability or integrity of Confidential Information, BOE Technology Assets or Processor Systems.

2. Confidentiality. Subject to any security review as required by the BOE Division of Instructional and Information Technology at its discretion, in furtherance of the use of Processor's software and/or services on behalf of the BOE (the "Services,") the Processor is permitted to Process the BOE's Confidential Information as set forth in the Service Description, attached hereto as Attachment A. In accordance with FERPA, the Processor agrees that to the extent that the Services relate to the Processor's Processing of Protected Information, the Services are (a) for the Processor to perform an institutional service or function for which the BOE would otherwise use its employees; or (b) in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. The Processor further agrees that it is hereby designated as the authorized representative of the BOE to the extent that the Services are in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. The Processor agrees to hold the Confidential Information in strict confidence, and not to disclose Confidential Information to or otherwise permit the Processing of Confidential Information by any other parties, nor Process such Confidential Information for the benefit of another or for any use or purpose other than for providing the Services. The confidentiality and data security obligations of the Processor under this Agreement shall survive any termination of this Agreement. The Processor agrees to conduct the Services in a manner that does not permit the personal identification of parents and students by anyone other than Authorized Users with legitimate interests in the Protected Information.

3. Authorized Users. The Processor shall only disclose Confidential Information to its employees ("Personnel"), and its nonemployee agents, assignees, consultants or subcontractors ("Non-Employee Processors," and together with Personnel, "Authorized Users") who need to Process the Confidential Information in order to carry out the Services and in those instances only to the extent justifiable by that need. The Processor shall ensure that all such Authorized Users comply with the terms of this Agreement. The Processor agrees that upon request by the BOE, it will provide the BOE with the names and affiliations of the Non-Employee Processors to whom it proposes to disclose, or has disclosed, Confidential Information. The Processor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this Agreement, shall apply to any Non-Employee Processor it engages to Process Confidential Information of the BOE. The Processor therefore agrees to ensure that each Non-Employee Processor is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this Agreement.

4. Compliance with Law.

(a) The Processor agrees to hold all Confidential Information it Processes in compliance with all applicable provisions of federal, state and local law, including but not limited to FERPA and New York Education Law §2-d and any applicable regulations promulgated thereunder. The Processor understands that the disclosure of Protected Information to persons or agencies not authorized to receive it is a violation of United States federal law and New York state law, which may result in civil and/or criminal penalties under New York State and Federal laws.

(b) In the event that disclosure of Confidential Information (including Protected Information) is required of the Processor under the provision of any law, judicial order or lawfully-issued subpoena, the Processor will (a) promptly notify the BOE of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the BOE to seek a protective order or to make any notifications required by law, and (b) disclose such Confidential Information only to the extent (i) allowed under a protective order, if any, or (ii) necessary to comply with the law or court order.

5. Mandatory N.Y. Education Law 2-d Requirements.

(a) BOE Data Privacy and Security Policies. The Processor agrees that it will comply with the BOE's data privacy and security policy, New York City Department of Education Chancellor's Regulation A-820, and any successor thereto.

(b) Subject Data Requests. If permitted by law, the Processor agrees to promptly notify the BOE of any requests it receives from parents, students, principals or teachers ("Subjects") or parties authorized by Subjects, to amend, inspect, obtain copies of, or otherwise access Protected Information in the possession or control of the Processor, in advance of compliance with such requests. The Processor shall defer to the judgment of the BOE in granting or denying such requests, and in confirming the identity of Subjects and the validity of any authorizations submitted to the Processor. The Processor agrees to assist the BOE in processing such requests in a timely manner, whether received by the Processor or by the BOE. The Processor shall amend any Protected Information in accordance with the BOE's decision and direction.

(c) Training. The Processor shall ensure that all Authorized Users with access to the Confidential Information are trained, prior to receiving such access, in their confidentiality and data security responsibilities under applicable law and understand the privacy and data security obligations of this Agreement. The Processor agrees to provide each Authorized User with data privacy and security training on a subsequent periodic basis during the period in which the Authorized User maintains such access.

(d) Privacy and Security Plan; Additional Data Privacy and Security Protections. The Processor shall neither retain nor incorporate any of the Confidential Information into any database or any medium other than may be required for it to provide the Services. The Processor agrees to maintain appropriate administrative, technical and physical safeguards in accordance with industry best practices and applicable law to protect the security, confidentiality and integrity of Protected Information in its custody. The Processor agrees to adhere to (a) its data privacy and security plan and the BOE Information Security Requirements (together, the "Plan"), attached hereto as Attachment B. The Processor warrants and represents that (i) its technologies, safeguards and practices, as outlined in the Plan, align with the NIST Cybersecurity Framework, and include sufficient (A) data privacy protections, including processes to ensure that personally identifiable information is not included in public reports or other public documents; and (B) data security protections, including data systems monitoring, encryption of data in motion and at rest, an incident response plan, limitations on access to Protected Information, safeguards to ensure Protected Information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of Protected Information when no longer needed; and (ii) its Plan meets all additional requirements of New York Education Law 2-d. The Processor agrees to use encryption technology to protect Protected Information while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the United States Department of Health and Human services in guidance issued under Section 13402(H)(2) of Public Law 111-5. The Processor acknowledges and agrees to conduct digital and physical periodic risk assessments and to remediate any identified security and privacy vulnerabilities in a timely manner. The BOE reserves the right to request information from the Processor regarding its security practices and compliance with the Plan, prior to authorizing any exchange of Confidential Information. The Processor shall conduct periodic digital and physical risk assessments and shall provide (a) a report to the BOE that describes any vulnerabilities identified through periodic network vulnerability scans, and (b) a remedial plan with associated timelines informing the BOE of all actions the Processor has taken or plans to take to rectify such vulnerabilities, in each case in a manner that would not further compromise data privacy or security. The BOE reserves the right to promptly terminate the Agreement with no further liability to the Processor, in the event that the Processor fails to comply with such risk mitigation plan or is unable to resolve its noncompliance with the Plan. The BOE may audit the Processor's Processing of the Confidential Information for data privacy and data security purposes, including but not limited to, the Processor's Plan, data privacy and security program and/or its information technology infrastructure or processes.

(e) Parent Bill of Rights. The Processor agrees to comply with the BOE Parents' Bill of Rights for Data Privacy and Security, attached hereto as Attachment C. The Processor shall complete the Supplemental Information section of Attachment C, and append it to this Agreement. The Processor shall notify the BOE on a yearly basis, by January 31 of each year that this Agreement remains in effect, of any change to its responses to Attachment C. The Processor acknowledges and agrees that the BOE shall make the Processor's Supplemental Information public, including but not limited to posting it on the BOE's website. The Processor acknowledges that this Agreement, including the attachments hereto, may be made available to the public.

(f) Reportable Data Events. The Processor shall promptly notify, without unreasonable delay (a) the BOE Office of Legal Services at 212-374-6888 and at studentprivacy@schools.nyc.gov (to the attention of the Chief Privacy Officer) and (b) the BOE Division of Information and Instructional Technology at data-security@schools.nyc.gov (to the attention of the Chief Information Security Officer) of (i) any unauthorized release or other Processing of Confidential Information, whether by the Processor, its Authorized Users or any other party that shall have gained access to the affected Confidential Information, or any other Security Incident; or (ii) any other breach of contractual obligations relating to data privacy and security under this Agreement or any other applicable Agreement (together with a Security Incident, a "Reportable Data Event"). In no event shall such notification occur more than twenty four (24) hours after confirmation of an event described in clause (i) of the previous sentence, or more than seventy-two (72) hours after confirmation of an event described in clause (ii) of the previous sentence. Such notification of the DOE shall summarize, in reasonable detail, the nature and scope of the Security Incident (including a description of all impacted DOE Data and DOE Technology Assets) and the corrective action already taken or planned by Processor, which shall be timely supplemented to the level of detail reasonably requested by the BOE, inclusive of relevant investigation or forensic reports. To the extent both (a) New York Education Law 2-d or any other law or regulation requires Subjects affected by the Reportable Data Event to be notified, and (b) the Reportable Data Event is not exclusively attributable to the acts or omissions of the BOE, the Processor shall be responsible, at its own cost and expense, to notify in writing all persons affected by the Reportable Data Event, or shall compensate the BOE for the full cost of any notifications that the BOE instead makes. The Processor agrees to assist and collaborate with the BOE in ensuring that required notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: (a) a brief description of the Reportable Data Event, the dates of the incident and the date of discovery, if known; (b) a description of the types of Confidential Information affected; (c) an estimate of the number of records affected; (d) a brief description of the investigation or plan to investigate; and (e) contact information for representatives who can assist parents or adult students that have additional questions. If requested, Processor shall provide the BOE with (a) physical access to the affected locations and operations within the control of Processor; (b) access to Processor's Authorized Users or other individuals with knowledge of the Reportable Data Event. The Processor shall fully cooperate with and assist the BOE in investigating the Reportable Data Event or in effectuating notifications, including, without limitation, by providing full access to any information, records or other material the BOE deems to be necessary for such purposes or required to comply with applicable law.

(g) No Sale or Commercial Use. The Processor agrees that it will not (i) sell Protected Information; (ii) use, disclose or otherwise Process Confidential Information for purposes of receiving remuneration, whether directly or indirectly; or (iii) use, disclose or otherwise Process Confidential Information for marketing, commercial or advertising purposes (or facilitate its Processing by any other party for such purposes), or to develop, improve or market products or services to students, or permit another party to do so.

6. Right to Termination. The BOE shall have the right at its sole discretion to terminate the Processor's access to the BOE's Confidential Information upon fifteen (15) days written notice to the Processor. The BOE shall have the right at its sole discretion to terminate the Processor's access to the BOE's Confidential Information immediately upon the Processor's breach of any confidentiality obligations herein. No claim for damages will be made or allowed to the Processor because of said termination.

7. Confidential Information Retention, Transfer and Destruction. Upon the earliest of any of the following (i) whenever requested by the BOE, (ii) whenever the Processor no longer needs the Confidential Information to provide the Services to the BOE, (iii) whenever a BOE school or office ceases use of a product or service of the Processor, with respect to the Confidential Information Processed for the school or office with respect to that product or service, or (iv) no later than upon termination of this Agreement, the Processor shall promptly (a) with respect to physical copies of Confidential Information, surrender, or if surrender is not practicable, securely delete or otherwise destroy Confidential Information and (b) with respect to digital and electronic Confidential Information, securely delete or otherwise destroy Confidential Information remaining in the possession of the Processor and its Authorized Users, including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data. The Processor shall ensure that no copies, summaries, or extracts of Confidential Information are retained on any storage medium whatsoever by the Processor or its Authorized Users. The Processor shall certify, in writing, that Confidential Information has been surrendered or destroyed in accordance with this Agreement via the "Certificate of Records Disposal" form attached to this Agreement as Attachment D. Any and all measures related to the extraction, deletion, transmission, destruction or disposition of Confidential Information will be accomplished utilizing an appropriate method of confidential destruction, including shredding, burning or certified/witnessed destruction of physical materials or verified erasure of magnetic media using approved methods of electronic file destruction. The Processor agrees not to attempt to re-identify, or have others attempt to re-identify, Subjects from any data remaining after such deletion, destruction or disposition. If student-, parent- or employee-generated content is stored or maintained by the Processor, Processor shall, at the request of the BOE, and if severable, transfer such student-generated content to a separate account, or multiple separate student accounts, accessible by the BOE. Processor shall transfer such content at any time required by the BOE, including but not limited to (a) upon termination of this Agreement or (b) upon a BOE's school or office's cessation of the use of a product or service of the Processor, with respect to that individual product or service. To the extent practicable, Processor shall not retain Protected Information of an individual Subject for more than one school year after the school year in which the data was received, unless further retention is required by the N.Y. State Retention Schedule LGS-1 or by applicable law, or unless its retention is requested by the BOE school or office that disclosed it.

8. BOE Property. All reports and work product containing Confidential Information (a) created or collected by the Processor, or (b) disclosed or transmitted to the Processor, pursuant to this Agreement, shall remain the exclusive property of the BOE. All rights, including the intellectual property rights in and to the Confidential Information Processed pursuant to this Agreement shall remain the exclusive property of the BOE. Any reports or work product may not contain any Confidential Information, unless required by the BOE or if necessary to carry out the Services.

9. Other Agreements. The Processor agrees that to the extent that any confidentiality or data security terms or conditions regarding the Services found in another agreement binding BOE employees, subcontractors, parents or students (together, "BOE Users,") including but not limited to any end-user license agreement, "click wrap," "click-through," "click and accept," "web-wrap," or other form of agreement requiring the individual user to accept terms in order to use or benefit from the Services, conflict with the terms found in this Agreement, the terms and conditions which afford more protection to BOE Users shall apply. Any subsequent agreements between the Processor and the BOE with respect to the provision of the Services shall include confidentiality and data security obligations on the part of the Processor at least as strict as set those forth in this Agreement. In the event a subsequent agreement fails to contain confidentiality and data security provisions with obligations at least as strict as this Agreement, the confidentiality provisions of this Agreement shall be deemed inserted therein, and shall continue to bind the Processor, unless such subsequent agreement specifically references this Agreement by name and disclaims its obligations in writing. To the extent that Processor's policies or practices conflict with the terms of this Agreement in a manner that diminishes the privacy and data security protections of BOE Users, the terms of this Agreement shall apply.

10. Other Terms.

(a) The Processor agrees that money damages would be an insufficient remedy for breach or threatened breach of this Agreement by the Processor. Accordingly, in addition to all other remedies that the BOE may have, the BOE shall be entitled to specific performance and injunctive or other equitable relief as a remedy for any breach of the confidentiality and other obligations of this Agreement.

(b) Nothing in this Agreement obligates either party to consummate a transaction, to enter into any agreement or negotiations with respect thereto, or to take any other action not expressly agreed to herein.

(c) The Processor shall defend, indemnify and hold harmless the BOE and the City of New York from any and all claims brought by third parties to the extent arising from, or in connection with, any negligent acts or omissions of the Processor and the Processor's Authorized Users or any other representatives for whom the Processor is legally responsible for, in connection with the performance of this Agreement (even if the allegations of the claims are without merit). Insofar as the facts or law relating to any of the foregoing would preclude the BOE, or its respective officials or employees from being completely indemnified by the Processor, the BOE and their respective officials and employees shall be partially indemnified by the Processor to the fullest extent permitted by law.

(d) No failure or delay (in whole or in part) on the part of either party hereto to exercise any right or remedy hereunder shall impair any such right or remedy, operate as a waiver thereof, or affect any right or remedy hereunder. All rights and remedies hereunder are cumulative and are not exclusive of any other rights or remedies provided hereunder or by law or equity. To the extent any provision of this Agreement is held to be unenforceable or invalid, the remainder of the Agreement shall be remain in full force and effect, and the Agreement shall be interpreted to give effect to the such provision to the maximum extent permitted by law.

(e) This Agreement shall be governed by and construed in accordance with the law of the State of New York. The Federal or State Courts of New York City, New York will have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement. This Agreement constitutes the entire Agreement with respect to the subject matter hereof; it supersedes any other Processor terms and conditions, all prior agreements or understandings of the parties, oral or written, relating to the Services and shall not be modified or amended except in writing signed by the Processor and the BOE. The Processor may not assign or transfer, without the prior written consent of the BOE, this Agreement. This Agreement shall inure to the benefit of the respective parties, their legal representatives, successors, and permitted assigns. This Agreement is effective upon execution of the Processor.

Signed and Agreed to:

Insert Processor Organization Name

By: ___________________________________

Date: __________________________________

Name: _________________________________

Title: __________________________________

Processor Acknowledgment

State of New York }
} ss.:
County of }

On this _____ day of ________________, 202__, before me, the undersigned, a Notary Public in and for said State, personally appeared one , personally known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her capacity, and that by his/her signature on the instrument, the entity or individual upon behalf of which the individual acted, executed the instrument.

____ NOTARY PUBLIC

Attachment A: Services Description

[INCLUDE DESCRIPTION OF SERVICES PURCHASED OR CONTRACTED FOR]

Attachment B: Processor Data Privacy and Security Plan

DOE Information Security Requirements Document to Be Inserted

Processor must also attach a Data Privacy and Security Plan, which at a minimum must address the following requirements:

(1) outline how Processor will implement all state, federal, and local data security and privacy contract requirements over the life of the agreement, consistent with NYC DOE's data security and privacy policy;

(2) specify the administrative, operational and technical safeguards and practices Processor has in place to protect the Protected Information that it will receive under the contract;

(3) demonstrate that it complies with the requirements of the NYC DOE's Parents' Bill of Rights for Data Privacy and Security;

(4) specify how officers or employees of the third-party contractor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

(5) specify if Processor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

(6) specify how the Processor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify NYC DOE;

(7) describe whether, how and when data will be returned to the NYC DOE, transitioned to a successor contractor, at the NYC DOE's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

Attachment C: BOE Parents' Bill of Rights for Data Privacy and Security

Both state and federal laws protect the confidentiality of information about your child that identifies him or her. Such information, which includes student-specific data, is known as "personally identifiable information." Under New York state's education law, if you are a parent of a child in the New York City public school district (the NYC DOE), you have the following rights regarding the privacy and security of your child's personally identifiable information and data.

(1) Your child's personally identifiable information cannot be sold or released for any commercial purposes.

(2) If your child is under age 18, you have the right to inspect and review the complete contents of your child's education records.

(3) Safeguards must be in place to protect your child's personally identifiable data when it is stored or transferred. These safeguards must meet industry standards and best practices. Examples of such safeguards include encryption, firewalls and password protection.

(4) You have the right to make complaints about possible breaches of student data and to have such complaints addressed. Complaints to the SED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. Complaints to the NYC DOE should be directed via email to studentprivacy@schools.nyc.gov, or in writing to the Office of the Chief Information Officer, the Division of Instructional and Information Technology, New York City Department of Education, 335 Adams Street, Brooklyn NY 11201.

(5) You have additional rights as a parent, including additional privacy rights under federal law. They are found in the NYC DOE's Parents' Bill of Rights and Responsibilities, available here: https://www.schools.nyc.gov/school-life/policies-for-all/parents-bill-of-rights

(6) You can find a complete list of all of the types of student data that the New York State Education Department (SED) collects at this web-link:
http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

You may also obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

Parents Bill of Rights for Data Privacy and Security—Supplemental Information

I. Explanation and Instructions

Pursuant to New York Education Law §2-d and 8 N.Y.C.R.R 121.3, the New York City Department of Education ("NYC DOE") is required to supplement its Parents Bill of Rights for Data Privacy and Security with additional information concerning a written agreement ("Agreement") under which an outside entity ("Entity") will receive personally identifiable information from education records of students ("PII"; see full definition below). In accordance with these provisions, it is necessary for you to provide a complete and accurate response to each item below. If an item is not applicable to your agreement with the NYC DOE, explain why. Your responses will be posted are subject to review and approval by the NYC DOE, and will be posted to the NYC DOE's website.

Please note that New York Education Law 2-d defines PII as follows:

1. With respect to student data, personally identifiable information from the DOE's education records, including but not limited to the following:
    a. The student's name;
    b. The name of the student's parent or other family members;
    c. The physical or electronic address, device number (including telephone and mobile phone numbers, geolocation information and IP addresses) and other contact information of the student or student's family;
    d. A personal identifier, such as the student's social security number, student number, or biometric record (including but not limited to fingerprints, facial images, iris scans and handwriting);
    e. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
    f. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty—including combinations of demographic, performance and school information that could lead to the student being identified); and
    g. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
2. With respect to teacher or principal data, any annual professional performance review (APPR) data disclosed by the DOE to the Entity on an identifiable basis.

Please note that "education records" include records directly related to a student and maintained by **or on behalf of** the DOE. Accordingly, to the extent the Entity is providing a service or function on behalf of the DOE, education records, and the PII found in it, includes information that the Entity may collect directly from parents or students.

With respect to any explanation the Entity provides below in response to the questionnaire:

- The NYC DOE reserves the right to review and reject them, or request further explanation. Note that certain options below match federal and state legal requirements, and deviations will need to be reviewed and considered on a case-by-case basis.
- Phrase your responses so that public posting of it will not jeopardize the security of PII or your data protection processes.

- Do not refer back to your written agreement with the NYC DOE, or use defined terms found elsewhere in the agreement or in other documents. Your explanations must stand on their own, since they will be posted publicly.
- Ensure that it is clear and uses plain English, because the audience for it consists of NYC DOE parents, staff, students and other interested members of the public.

II. Questionnaire

1. Name of Entity

Click or tap here to enter text.

2. Type of Entity

☐ Commercial Enterprise

☐ Research Institution or Evaluator

☐ Community Based Organization or Not-for-Profit

☐ Government Agency

☐ Other (You must explain below)
Click or tap here to enter text.

3. Contract / Agreement Term

☐ The Agreement has a Start Date: Click or tap here to enter text.
☐ The Agreement has an End Date: Click or tap here to enter text.

☐ The Agreement covers multiple products, services and/or DOE schools and offices, and so Start and End Dates vary by product, service, and DOE schools and/or offices.

4. Description of the exclusive purpose(s) for which Entity will receive/access PII

Describe briefly the project/evaluation/research you are conducting or participating in, and/or the commercial product or service you are providing. Describe the purposes for which you are receiving or accessing PII.
Click or tap here to enter text.

5. Type of PII that the Entity will receive/access

Check all that apply:

☐ Student PII

☐ APPR PII (Identifiable Teacher or Principal Annual Professional Performance Review Data)

☐ Entity will not receive or access PII (do not choose this response if Entity's services or products permit users to store PII on a platform that the Entity or its subcontractors host)

☐ Other (You must explain below)
Click or tap here to enter text.

6. Subcontractor Written Agreement Requirement

In accordance with New York Education Law 2-d, the Entity may not share PII with subcontractors without a written agreement that requires each of its subcontractors to adhere to, at a minimum, materially similar—and no less protective—data protection obligations imposed on the Entity by the Agreement with the NYC DOE and by applicable state and federal laws and regulations.

Check one option only:

☐ The Entity will not share PII with subcontractors, outside persons, or third party entities.

☐ The Entity will utilize subcontractors or third party entities (including any cloud services providers) and agrees not share PII unless similar data protection obligations contained herein are imposed on each subcontractor or third party, in compliance with applicable New York State and federal law and using industry standard best practices for data privacy and security.

☐ Other (You must explain below)
Click or tap here to enter text.

7. Data Transition and Secure Destruction

Upon expiration or termination of the Agreement, the Entity shall (check all that apply):

☐ Securely transfer PII to NYC DOE, or a successor contractor at the NYC DOE's option and written discretion, in a format agreed to by the parties

☐ Securely delete and/or destroy PII

☐ Other (You must explain below)

Click or tap here to enter text.

8. Challenges to Data Accuracy

In accordance with N.Y. Education Law 2-d, parents, students, eligible students, teachers, or principals may seek copies of their PII, or seek to challenge the accuracy of PII in the custody or control of the Entity. Typically, they can do so by contacting the NYC DOE using the email address or mailing address below. If a correction to PII is deemed necessary, the Entity agrees to facilitate such corrections within 21 days of receiving the NYC DOE's written request. The Entity must forward the request to the NYC DOE as soon as practicable in order for the DOE to authenticate the identity of the student or parent, and to advise the Entity on how to process the request.

All requests for copies of PII or requests to challenge the accuracy of PII should be directed to the following email address: studentprivacy@schools.nyc.gov or in writing to the Office of the Chief Information Officer, the Division of Instructional and Information Technology, New York City Department of Education, 335 Adams Street, Brooklyn NY 11201.

Please select one option only:

☐ The Entity agrees to the procedure outlined above

☐ Other (You must explain below)

Click or tap here to enter text.

9. Security and Storage Protections

Describe where PII will be stored or hosted (check all that apply)

☐ Using a cloud or infrastructure owned tool hosted by a subcontractor; i.e., Click or tap here to enter text. **(Please enter the name of the cloud services provider and the cloud services solution)**

☐ Using an Entity-owned and/or internally hosted-solution

☐ No PII will be stored or hosted by Entity

☐ Other (you must explain below):

Click or tap here to enter text.

10. Describe the administrative, technical and/or physical safeguards to ensure PII will be protected and how the Entity will mitigate data privacy and security risks. (Please do so in a manner that ensures that disclosure of the description on NYC DOE's website will not compromise the security of the data or the Entity's security practices and protocols):

Click or tap here to enter text.

11. Encryption

Pursuant to New York Education Law 2-d, PII must be encrypted while in motion and while at rest. By checking the box below, Entity agrees that PII will be encrypted using industry standard data encryption technology while Protected Information is in motion and at rest.

☐ Entity agrees that PII will be encrypted in motion and at rest using industry-standard data encryption technology.

☐ Other (you must explain below):

Click or tap here to enter text.

Attachment D: Certificate of Records Disposal

CERTIFICATE OF RECORDS DISPOSAL

□ **The information described below was destroyed in the normal course of business pursuant to organizational retention schedule destruction policies and procedures, and/or written agreement.**

Description of Information Disposed Of/Destroyed:
□ Noted in Attachment

PERSON PERFORMING SANITIZATION

Name:	Title:	
Organization:	Location:	Phone:

MEDIA INFORMATION

Make/Vendor:	Model Number:
Serial Number(s)/Property Numbers:	
Media Type:	Source (i.e., user name/property #):
Data Classification:	Data Backed up? □ Yes □ No □ Unknown
Backup Location (if applicable):	

SANITIZATION DETAILS

Method Type:	□ Clear	□ Purge	□ Damage	□ Destruct	□ Other:
Method Used:	□ Degauss	□ Overwrite	□ Block Erase	□ Crypto Erase	□ Other:

Method Details:

Tool Used (include version):

Verification Method: □ Full □ Quick Sampling □ Other:

Post-Sanitization Classification:

Notes:

MEDIA DESTINATION

□ Internal Reuse □ External Reuse □ Recycling Facility □ Manufacturer □ Other (specify in Details)

Details:

SIGNATURE

□ I attest that the information provided on this Certification of Destruction and Sanitization is accurate to the best of my knowledge.

Signature: Date:

VALIDATION

Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date: