

Data Privacy Agreement

New York Education Law § 2-d Third-Party Contractor Rider | Template v1.0

This Data Privacy Agreement ("Agreement") is entered into as of [EFFECTIVE DATE] between The Summit School (Queens), an approved private school for the education of students with disabilities located at 187-30 Grand Central Parkway, Jamaica Estates, NY 11432 ("Summit" or "Educational Agency"), and [CONTRACTOR LEGAL NAME], with offices at [CONTRACTOR ADDRESS] ("Contractor"). This Agreement supplements the agreement between the parties dated [DATE] for [PRODUCT/SERVICE] (the "Service Agreement"). In the event of a conflict between this Agreement and the Service Agreement or any Contractor terms of service, this Agreement controls with respect to Protected Data.

1. Definitions

Protected Data	Student Data and Teacher or Principal Data, as defined in Education Law § 2-d and 8 NYCRR § 121.1, and any other personally identifiable information about students, parents, or Summit staff that Contractor receives from or on behalf of Summit, or that is generated by the Services in a form identifiable to an individual.
Student Data	Personally identifiable information, as defined in FERPA (34 CFR § 99.3), from the student records of Summit.
Teacher or Principal Data	Personally identifiable information from records relating to annual professional performance reviews, to the extent any exists.
Breach	The unauthorized acquisition, access, use, or disclosure of Protected Data by or to a person not authorized to acquire, access, use, or receive it.
Subcontractor	Any person or entity, including affiliates and hosting providers, engaged by Contractor to perform any part of the Services involving Protected Data.
Services	The products and services described in Exhibit A.

2. Purpose and ownership

Contractor will receive Protected Data solely for the exclusive purposes described in Exhibit A. All Protected Data remains the property of, and under the control of, Summit and the placing school district(s). Contractor acquires no rights in Protected Data other than the limited license to use it to perform the Services.

3. Contractor obligations (Education Law § 2-d(5) and 8 NYCRR § 121.9)

Contractor represents, warrants, and agrees that it will:

1. Comply with Education Law § 2-d, 8 NYCRR Part 121, FERPA, IDEA, COPPA (where applicable), the NY SHIELD Act, and Summit's Data Privacy and Security Policy, and be bound by the Summit Parents' Bill of Rights for Data Privacy and Security attached as Exhibit C.
2. Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework.
3. Limit internal access to Protected Data to those employees or Subcontractors who need such access to provide the Services, and who have been trained on the federal and state laws governing confidentiality of such data.
4. Not use Protected Data for any purpose other than those explicitly authorized in Exhibit A, and not use it to develop, train, or improve products or services, including artificial intelligence or machine-learning models, except as strictly necessary to provide the Services to Summit **[and only in de-identified, aggregated form if expressly permitted in Exhibit A]**.
5. Not disclose Protected Data to any other party without the prior written consent of the parent or eligible student, unless the disclosure is required by statute or court order and Contractor provides Summit notice no later than the time of disclosure, unless such notice is expressly prohibited.
6. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.
7. Use encryption to protect Protected Data in motion and at rest, in accordance with 8 NYCRR § 121.1 and industry standards (TLS 1.2 or higher in transit; AES-256 or equivalent at rest).
8. Not sell Protected Data, and not use or disclose it for any marketing or commercial purpose, or permit any other party to do so. Contractor will not use Protected Data to target advertising to students, parents, or staff.
9. Not attempt to re-identify de-identified data, and not transfer de-identified data to any party unless that party agrees not to attempt re-identification.
10. Ensure that any Subcontractor with access to Protected Data is bound by written agreement to obligations no less protective than this Agreement, remain fully responsible for Subcontractors' performance, and provide Summit a current list of Subcontractors on request and notice of changes.
11. Notify Summit of any Breach, in the most expedient way possible and without unreasonable delay, and in no event later than seven (7) calendar days after discovery, as set out in Section 5.
12. Cooperate with Summit and law enforcement in the investigation of any Breach, and reimburse Summit for the full cost of any notifications to parents, eligible students, staff, or regulators required as a result of a Breach attributable to Contractor or its Subcontractors (Education Law § 2-d(6)(c)).
13. Provide a Data Security and Privacy Plan meeting 8 NYCRR § 121.6, attached as Exhibit B, and comply with it throughout the term.
14. Make Protected Data available to Summit for inspection, correction, or export on request, and correct inaccurate Protected Data as directed by Summit within **[10]** business days.
15. On request, make available to Summit reasonable evidence of compliance, such as current SOC 2 Type II reports, ISO 27001 certificates, penetration-test summaries, or completed security questionnaires.

4. Parents' Bill of Rights and supplemental information

Contractor acknowledges receipt of the Summit Parents' Bill of Rights for Data Privacy and Security (Exhibit C) and agrees that Summit will publish on its website the supplemental information required by 8 NYCRR § 121.3(c), including the information in Exhibit A, and a summary of Contractor's Data Security and Privacy Plan.

5. Breach notification

Contractor's notification of a Breach will be made to the Summit Data Protection Officer at privacy@summitqueens.com, will describe the nature of the Breach, the Protected Data involved, the dates of the Breach and its discovery, the steps taken and planned to remediate, and a contact person. Contractor will provide updates as its investigation proceeds. Contractor will not notify affected individuals, placing school districts, or regulators directly unless directed by Summit or required by law, and will cooperate with Summit's notifications to the NYSED Chief Privacy Officer (within 10 calendar days) and to affected persons (within 60 calendar days) under 8 NYCRR § 121.10.

6. Term, return, and destruction of data

This Agreement is effective on the Effective Date and remains in effect for as long as Contractor holds any Protected Data. Upon expiration or termination of the Service Agreement, or on Summit's earlier written request, Contractor will (a) return Protected Data to Summit in a commercially reasonable, usable format within [30] days, and (b) securely delete or destroy all Protected Data in its and its Subcontractors' possession, including in backups, within [90] days, using methods consistent with NIST SP 800-88, and (c) certify such destruction in writing on request. Contractor may retain Protected Data only to the extent required by law, and this Agreement continues to govern any retained data.

7. Compliance, audit, and remedies

Summit may, on reasonable notice, review Contractor's compliance with this Agreement through questionnaires, review of third-party audit reports, or, where a material concern exists, an on-site or virtual assessment. Contractor's breach of this Agreement is a material breach of the Service Agreement and may result in termination for cause without penalty to Summit. Contractor acknowledges that violations of Education Law § 2-d may subject it to civil penalties and to prohibition from accessing student data from educational agencies in New York under 8 NYCRR § 121.11. Contractor will indemnify and hold harmless Summit from claims, fines, and costs arising from Contractor's or its Subcontractors' breach of this Agreement.

8. General

This Agreement is governed by the laws of the State of New York. Any modification must be in writing signed by both parties. If any provision is held unenforceable, the remainder continues in effect. Contractor may not assign this Agreement without Summit's written consent. Contractor terms of service, privacy policies, or "click-through" terms that conflict with this Agreement have no effect with respect to Protected Data.

Signatures

The Summit School (Queens)	[CONTRACTOR LEGAL NAME]
By: _____	By: _____
Name: [NAME]	Name: [NAME]
Title: [Executive Director / Director]	Title: [TITLE]
Date: _____	Date: _____

Exhibit A — Services and supplemental information

To be completed by Contractor and Summit. This information will be published on Summit's website pursuant to 8 NYCRR § 121.3(c).

Product / service	[Name and description]
Exclusive purposes for which Protected Data is used	[Specific school functions]
Protected Data elements to be shared	[List every element]
Population	[Students / parents / staff; grades or programs]
Subcontractors and hosting provider	[Names and roles; link to subprocessor list]
Term of Service Agreement	[Start] – [End]; renewal terms
Disposition of data at expiration	[Return format; deletion timeline; certification]
Process for challenging accuracy of data	Written request to Summit DPO; Contractor corrects as directed within [10] business days.
Data storage location	[Provider and region — must be in the United States unless Summit agrees otherwise in writing]
Encryption in transit / at rest	[Protocols and standards]
De-identified or aggregate data use permitted?	[No / Yes, describe]

Exhibit B — Contractor Data Security and Privacy Plan

Pursuant to 8 NYCRR § 121.6, Contractor must describe how it will meet each of the following. Contractor may attach existing policies or audit reports in place of narrative responses where they address the item.

1. Legal and policy compliance	How Contractor will implement all state, federal, and local data security and privacy requirements, including Education Law § 2-d, Part 121, FERPA, and Summit's Data Privacy and Security Policy, over the life of the contract. [Contractor response]
2. Administrative, operational, and technical safeguards	The safeguards and practices Contractor has in place, aligned with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover), including access control, MFA, logging and monitoring, vulnerability and patch management, secure development, and business continuity. [Contractor response]
3. Demonstrating compliance	How Contractor will demonstrate compliance, e.g., SOC 2 Type II reports, ISO 27001 certification, annual security questionnaires, penetration-test attestations. [Contractor response]
4. Employee training	How and when Contractor trains its officers and employees with access to Protected Data on the federal and state laws governing confidentiality, and how completion is tracked. [Contractor response]
5. Subcontractor management	How Contractor ensures Subcontractors abide by the same data protection and security requirements, including contractual flow-down and due diligence. [Contractor response]
6. Incident management	Contractor's procedures for managing data security and privacy incidents affecting Protected Data, including detection, containment, investigation, and notification to Summit within seven (7) calendar days. [Contractor response]
7. Data return and destruction	How Contractor will return, delete, or destroy Protected Data at expiration or termination, including from backups, and certify destruction. [Contractor response]
8. Encryption	Encryption standards used for Protected Data in transit and at rest, and key-management practices. [Contractor response]
9. Parents' Bill of Rights	Contractor's acknowledgment that it has received and will comply with the Summit Parents' Bill of Rights (Exhibit C). [Contractor acknowledgment / signature]

Exhibit C — Summit Parents' Bill of Rights for Data Privacy and Security

[Attach the current published Parents' Bill of Rights.]