

Third-Party Contractor Supplemental Information

Appendices to the Parents' Bill of Rights for Data Privacy and Security | Last updated: September 2026

Summit publishes the following supplemental information for each third-party contractor that receives personally identifiable information, as required by 8 NYCRR § 121.3(c). Each sheet follows the (A)–(F) format set out in Section 10 of the Bill of Rights.

1. Google	Google Workspace for Education
2. Anthropic	Claude for Enterprise

Supplemental Information for Third-Party Contract

Appendix to the Parents' Bill of Rights for Data Privacy and Security (8 NYCRR § 121.3(c))

Third-Party Contractor	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043
Contract / Service	Google Workspace for Education — Gmail, Drive, Docs/Sheets/Slides, Classroom, Calendar, Meet, and Chat for students and staff
Data shared	Student and staff names, school-issued email addresses and usernames, organizational unit and grade grouping, and content users create or store in the services (documents, assignments, messages, files), which may include education records
Population	All students and staff (Summit's primary platform for email, classwork, and files)
Agreement / term	Ongoing subscription under the Google Workspace for Education Terms of Service; Data Processing Amendment accepted

(A) Exclusive purpose(s) for which the data will be used

Data is used solely to provide school-managed email, document creation and storage, classroom collaboration, and communication tools for students and staff. Under the Google Workspace for Education Terms of Service and Data Processing Amendment, Google processes Summit customer data only to provide the core services, does not serve advertising in the core services, and does not use core-service data for advertising purposes or to build student profiles.

(B) Subcontractors / further disclosure

Google's agreement requires that any subprocessor engaged to process customer data be bound by written obligations providing at least the same level of data protection. Google publishes its list of Google Workspace subprocessors and provides notice of changes. Summit administrators control which additional Google services are enabled for student accounts and restrict sharing of data outside the Summit domain.

(C) Duration of agreement and data disposition upon expiration

The subscription is ongoing and renews annually; Summit may terminate at any time and may export all customer data at any time. Upon termination, Google deletes customer data from its systems within the period specified in its Data Processing Amendment (generally within 180 days of deletion by the customer or termination), including from backups.

(D) Right to challenge accuracy

A parent, student, or eligible student who believes data collected is inaccurate may request a correction by contacting Summit's Data Protection Officer at privacy@summitqueens.com. Requests will be reviewed in accordance with Summit's record-amendment procedures under FERPA (34 CFR §§ 99.20–99.22) and Education Law § 2-d. Summit makes corrections directly in the system or directs the contractor to do so; parents do not need to contact the contractor.

(E) Where the data is stored

Data is stored in Google-owned and operated data centers, which are located in the United States and other countries, subject to the protections of the Data Processing Amendment.

(F) Security protections in place

Data is encrypted in transit (TLS) between users and Google and between Google data centers, and at rest using AES-256 or stronger. Google Workspace maintains ISO/IEC 27001, 27017, and 27018 certifications and SOC 2/SOC 3 attestations and a security program aligned with the NIST Cybersecurity Framework. Summit enforces 2-step verification for staff, restricts external sharing, limits student accounts to approved services, and manages all accounts through the Admin console. Google must notify Summit of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay, and in no case later than seven (7) calendar days after discovery, as required by 8 NYCRR § 121.10.

This supplemental information is based on representations made in Google's Data Security and Privacy Plan, contract, and published security documentation, and is reviewed annually by Summit's Data Protection Officer.

Supplemental Information for Third-Party Contract

Appendix to the Parents' Bill of Rights for Data Privacy and Security (8 NYCRR § 121.3(c))

Third-Party Contractor	Anthropic, PBC, 548 Market Street, San Francisco, CA 94104
Contract / Service	Claude for Enterprise — AI assistant used by authorized staff for document drafting, data formatting, and administrative automation
Data shared	Only the data authorized staff include in prompts and uploaded files, which may include student names, identification numbers, grades, and schedules. Summit policy requires de-identification (identification number or code in place of name) wherever a task does not require the name; IEPs, evaluations, and health or behavioral records are not processed.
Population	Students whose records are processed by authorized staff; staff users
Agreement / term	Enterprise agreement in progress — not in use with student information until the Data Privacy Agreement is signed

(A) Exclusive purpose(s) for which the data will be used

Data is used solely to provide the Claude for Enterprise service to Summit's authorized users. Under Anthropic's Commercial Terms of Service and Data Processing Addendum, Anthropic does not train its models on Summit's inputs or outputs and processes customer content only to provide, maintain, and secure the service, to enforce its usage policies, and as required by law.

(B) Subcontractors / further disclosure

Anthropic engages subprocessors (cloud infrastructure providers) solely as necessary to deliver the service and requires them by written agreement to protect customer data consistent with Anthropic's DPA. Anthropic publishes its subprocessor list and provides notice of changes.

(C) Duration of agreement and data disposition upon expiration

The Enterprise agreement is annual and renews each year. Organization administrators control data retention settings. Upon termination, Anthropic deletes customer data within the period specified in its DPA, including from backups. Summit administrators may delete conversations and projects at any time.

(D) Right to challenge accuracy

A parent, student, or eligible student who believes data collected is inaccurate may request a correction by contacting Summit's Data Protection Officer at privacy@summitqueens.com. Requests will be reviewed in accordance with Summit's record-amendment procedures under FERPA (34 CFR §§ 99.20–99.22) and Education Law § 2-d. Summit makes corrections directly in the system or directs the contractor to do so; parents do not need to contact the contractor.

(E) Where the data is stored

Data is stored in Anthropic's cloud infrastructure located in the United States.

(F) Security protections in place

Data is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256). Anthropic maintains SOC 2 Type II and ISO/IEC 27001 attestations and supports single sign-on, domain capture, role-based administration, and audit logs for Enterprise organizations. Summit restricts Claude use with student data to Enterprise seats under the signed agreement, prohibits use of personal or consumer AI accounts for any Summit PII, and requires de-identified inputs where possible. Anthropic must notify Summit of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay, and in no case later than seven (7) calendar days after discovery, as required by 8 NYCRR § 121.10.

Post this sheet and list Anthropic on the website only after the Enterprise agreement and Data Privacy Agreement are signed. This supplemental information is based on representations made in Anthropic's Data Security and Privacy Plan, contract, and published security documentation, and is reviewed annually by Summit's Data Protection Officer.