

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. PowerSchool	PowerSchool Student Information System (SIS) with PowerTeacher Pro
2. Google	Google Workspace for Education
3. Microsoft	Microsoft 365 for staff
4. Orah	Orah student life platform for the residence
5. Airtable	Airtable cloud database
6. Intuit	QuickBooks Online
7. Adobe	Adobe Creative Cloud for Education
8. Brivo	Brivo Access cloud-based door access control for staff credentials
9. Singlewire	InformaCast emergency mass notification for staff (paging, phone, SMS, email, and mobile app alerts)
10. CENTEGIX	CENTEGIX CrisisAlert
11. Anthropic	Claude for Enterprise
12. monday.com	monday.com work management

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	PowerSchool Group LLC, 150 Parkshore Drive, Folsom, CA 95630
Contract / Service	PowerSchool Student Information System (SIS) with PowerTeacher Pro — student enrollment, scheduling, attendance, gradebook, report cards, IEP document attachments, and district reporting
Data shared	Student name, local and NYSSIS/district identification numbers, date of birth, gender, address, parent/guardian names and contact information, placing district and program, enrollment dates, class schedules, attendance, grades and assessments, behavior incidents where recorded, IEP documents and classification, and health/emergency information where entered; staff names and school email addresses
Population	All enrolled students; teaching and administrative staff
Agreement / term	Annual subscription, renewed each school year; Data Privacy Agreement on file

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

Student data is used solely to provide student information system services to Summit: maintaining enrollment records, scheduling, attendance, the PowerTeacher Pro gradebook, report cards, IEP and related document storage, parent/guardian contacts, and state and district reporting for students enrolled at Summit. PowerSchool may use PII only to provide, support, and secure the contracted services. Data is not used for any other purpose, including marketing, advertising, profiling, or product development.

(B) Subcontractors / further disclosure

PowerSchool may share data with its cloud hosting and infrastructure subcontractors solely as necessary to deliver the contracted service. Every such subcontractor is contractually bound to the same data protection and confidentiality obligations imposed on PowerSchool under its agreement with Summit, including Education Law § 2-d, Part 121, and FERPA requirements, restrictions on use and disclosure, and required security safeguards. PowerSchool discloses its subprocessors in its Data Privacy Agreement.

(C) Duration of agreement and data disposition upon expiration

The agreement is an annual subscription renewed each school year. Upon expiration or termination, PowerSchool returns Summit's data in a usable export format on request and securely destroys all student data in its possession, including backups, within the period specified in the Data Privacy Agreement, except where retention is required by law, and provides written confirmation of destruction on request.

(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@summitnyack.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

Student data is stored in PowerSchool's cloud environment on Amazon Web Services data centers 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). Access is restricted to authorized personnel through role-based access controls and multi-factor authentication. PowerSchool maintains a security program aligned with the NIST Cybersecurity Framework, undergoes independent SOC 2 audits, and maintains a documented incident response plan. On Summit's side, staff access is limited by security group to those with a legitimate educational interest, and multi-factor authentication is enforced for staff logins. PowerSchool 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 PowerSchool'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	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	Students with Summit accounts; all staff
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@summitnyack.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	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Contract / Service	Microsoft 365 for staff — Entra ID (identity), Exchange Online, OneDrive, SharePoint, Teams, and Office applications. Students do not have Microsoft accounts.
Data shared	Staff names, school-issued email addresses, directory attributes (role, group, department), and content staff create or store in the services (email, files, Teams messages). Because staff use these tools to do their work, files and email may incidentally contain student education records.
Population	Staff only
Agreement / term	Annual education subscription, renewed each school year; Microsoft Data Protection Addendum accepted

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

Data is used solely to provide identity and account management, email, file storage, collaboration, and productivity tools for Summit staff. Under the Microsoft Product Terms and Data Protection Addendum (DPA), Microsoft processes customer data only to provide the services and for compatible business operations, and does not use it for advertising or profiling.

(B) Subcontractors / further disclosure

Microsoft's DPA requires subprocessors that access customer data to be bound by written obligations at least as protective as the DPA. Microsoft publishes its list of online services subprocessors and provides advance notice of additions.

(C) Duration of agreement and data disposition upon expiration

The subscription is annual and renews each school year. Summit may export all customer data at any time. Upon expiration or termination, Microsoft retains customer data in a limited-function account for 90 days to allow extraction, after which it is deleted within the period specified in the DPA (generally within 180 days), 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@summitnyack.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 Microsoft data centers located in the United States for Summit's U.S.-based tenant, per Microsoft's published data residency commitments for core Microsoft 365 services.

(F) Security protections in place

Data is encrypted in transit (TLS 1.2 or higher) and at rest (BitLocker volume encryption and service-level encryption, AES-256). Microsoft 365 maintains ISO/IEC 27001 and 27018 certifications, SOC 1/2/3 attestations, and FedRAMP authorization, and a security program aligned with the NIST Cybersecurity Framework. Summit enforces multi-factor authentication and conditional access through Entra ID and role-based administration. Microsoft 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.

Microsoft 365 is a staff-only system at Summit. This sheet is kept on file because staff email and files may incidentally contain student records. This supplemental information is based on representations made in Microsoft'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	Boardingware International Ltd., trading as Orah (Auckland, New Zealand)
Contract / Service	Orah student life platform for the residence — attendance and roll checks, leave and sign-in/out, pastoral notes, and parent/guardian communication
Data shared	Student name, photo, date of birth, grade and residence assignment, attendance and location status, leave requests, pastoral and residential notes, medical alerts entered by staff, and parent/guardian names and contact details; staff names and roles
Population	Residential students; residential and supervisory staff; parents/guardians
Agreement / term	Annual subscription, renewed each school year; Data Privacy Agreement on file

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

Data is used solely to provide residential student management services to Summit: tracking student attendance, location, and leave; recording pastoral and residential notes; and communicating with parents/guardians and staff about student welfare. Orah may use PII only to provide, support, and secure the contracted service and for no other purpose, including marketing, advertising, or profiling.

(B) Subcontractors / further disclosure

Orah shares data with its cloud hosting provider (Amazon Web Services) and other subprocessors solely as necessary to deliver the contracted service. Every such subcontractor is contractually bound to the same data protection and confidentiality obligations imposed on Orah under its agreement with Summit. Orah discloses its subprocessors in its privacy documentation.

(C) Duration of agreement and data disposition upon expiration

The agreement is an annual subscription renewed each school year. Upon expiration or termination, Orah provides an export of Summit's data on request and securely destroys all student data in its possession, including backups, within the period specified in the Data Privacy Agreement, except where retention is required by law, and confirms destruction in writing on request.

(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@summitnyack.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

Student data is stored on Amazon Web Services infrastructure in the United States hosting region selected for Summit's account.

(F) Security protections in place

Data is encrypted in transit (TLS, with automatic redirection to secure connections) and at rest on Orah's servers. Orah holds ISO/IEC 27001 and ISO/IEC 27018 certifications, is a Student Privacy Pledge signatory, and maintains 24/7 monitoring, automated daily backups, granular role-based access controls, and an incident response program. Summit limits Orah access to residential and supervisory staff with a legitimate need. Orah 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 Orah'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	Airtable, Inc., 799 Market Street, San Francisco, CA 94103
Contract / Service	Airtable cloud database — internal administrative tracking for admissions, enrollment, and program records
Data shared	Student name, identification number, grade, placing district, program, key dates, parent/guardian contact information, and administrative notes, limited to the fields needed for each tracking base
Population	Students in the tracking bases; staff users
Agreement / term	Annual subscription, renewed each school year; Airtable Data Processing Addendum accepted

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

Data is used solely to support Summit's internal administrative workflows. Airtable, as the platform provider, processes Summit's content only to provide, support, and secure the service and for no other purpose, including marketing, advertising, or training of models on Summit content; Summit keeps Airtable's AI features disabled for bases containing student data.

(B) Subcontractors / further disclosure

Airtable engages subprocessors, including its cloud hosting provider (Amazon Web Services), solely as necessary to deliver the service. Airtable's Data Processing Addendum requires subprocessors to be bound by written obligations at least as protective as Airtable's own, and Airtable publishes its subprocessor list with notice of changes.

(C) Duration of agreement and data disposition upon expiration

The subscription is annual and renews each school year. Summit may export all bases at any time. Upon termination, Airtable deletes customer content within the period specified in its Data Processing Addendum, 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@summitnyack.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 Airtable's production environment hosted on Amazon Web Services data centers 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). Airtable maintains SOC 2 Type II and ISO/IEC 27001 attestations, role-based permissions, two-factor authentication, and an incident response program. Summit restricts base and workspace sharing to authorized staff and does not use public share links for bases containing PII. Airtable 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 Airtable'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	Intuit Inc., 2700 Coast Avenue, Mountain View, CA 94043
Contract / Service	QuickBooks Online — accounting, tuition and service billing to placing districts and agencies, accounts payable, and payroll
Data shared	Student data limited to what is needed to invoice districts for tuition and services: student name, placing school district or agency, program or placement type, dates of service, and billed amounts. Staff and vendor data: employee names, addresses, Social Security numbers, bank account details, and compensation for payroll.
Population	All enrolled students (billing records only); employees; vendors; placing districts
Agreement / term	Ongoing subscription; Intuit business-customer terms and Data Processing Agreement accepted

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

Data is used solely to provide accounting, invoicing, and payroll services to Summit, including preparing and tracking tuition and service invoices to placing school districts and agencies for each enrolled student. Intuit may use data only to provide, support, and secure the contracted services and as described in its business-customer terms, and not for marketing to students or parents or for building profiles. Summit limits student data in QuickBooks to the minimum needed for billing — no grades, IEP, health, or behavioral information is entered.

(B) Subcontractors / further disclosure

Intuit engages subprocessors (hosting, payment processing, payroll tax filing) solely as necessary to deliver the services and requires them to maintain security and confidentiality obligations consistent with Intuit's own. Intuit describes its service providers in its privacy documentation.

(C) Duration of agreement and data disposition upon expiration

The subscription is ongoing and renews automatically. Summit may export its company file and reports at any time. Upon cancellation, Intuit retains read-only access to data for one year, after which data is deleted in accordance with Intuit's retention policy, except where retention is required by law (for example, tax and payroll records). Summit retains billing records for the period required by its records retention schedule and audit requirements.

(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@summitnyack.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 Intuit-managed data centers and cloud infrastructure located in the United States.

(F) Security protections in place

Data is encrypted in transit (TLS) and at rest (AES-256). Intuit maintains SOC 1 and SOC 2 attestations, multi-factor authentication, role-based user permissions, and an incident response program. Summit restricts QuickBooks access to business-office staff, enforces multi-factor authentication, and limits student fields to name, district, program, and service dates. Because staff Social Security and bank account numbers are “private information” under the NY SHIELD Act, Summit treats any breach as reportable under GBL § 899-aa as well as Education Law § 2-d. Intuit 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 Intuit'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	Adobe Inc., 345 Park Avenue, San Jose, CA 95110
Contract / Service	Adobe Creative Cloud for Education — creative and document tools for students and staff, managed through the Adobe Admin Console
Data shared	Student and staff names, school email addresses, and content created or stored in Adobe cloud services (documents, images, projects). Student accounts are provisioned by Summit as managed education accounts, not personal Adobe IDs.
Population	Students in creative arts and technology programs; staff
Agreement / term	Annual education license, renewed each school year; Adobe Data Processing Agreement accepted

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

Data is used solely to provision and operate licensed Adobe applications and cloud storage for Summit users. Under the Adobe education terms and Data Processing Agreement, Adobe processes customer content only to provide the services; content-analysis and product-improvement features are disabled for K-12 education accounts, and Adobe does not use K-12 student data for advertising or profiling.

(B) Subcontractors / further disclosure

Adobe uses subprocessors, including cloud hosting providers, solely as necessary to deliver the services, and requires them by written agreement to protect personal data consistent with Adobe's DPA. Adobe publishes its subprocessor list and provides notice of changes.

(C) Duration of agreement and data disposition upon expiration

The license is annual and renews each school year. Summit administrators may remove users and export content at any time. Upon termination, Adobe deletes customer content within the period specified in its Data Processing Agreement, 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@summitnyack.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 Adobe cloud infrastructure on data centers 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). Adobe maintains SOC 2 Type II and ISO/IEC 27001 certifications under the Adobe Common Controls Framework and supports single sign-on through Summit's identity provider. Summit provisions students only with managed education accounts, restricts sharing features, and removes accounts at withdrawal. Adobe 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 Adobe'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	Brivo Systems LLC, 7700 Old Georgetown Road, Bethesda, MD 20814
Contract / Service	Brivo Access cloud-based door access control for staff credentials
Data shared	Staff and contractor names, credential/badge numbers, group and schedule assignments, and door access event history. Students are not issued credentials.
Population	Staff and contractors
Agreement / term	Annual subscription, renewed each school year

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

Data is used solely to operate Summit's physical access control system: managing credentials, controlling door access, and logging access events for safety and security. Brivo may use PII only to provide, support, and secure the service and for no other purpose.

(B) Subcontractors / further disclosure

Brivo engages its cloud hosting provider (Amazon Web Services) and support subcontractors solely as necessary to deliver the service and requires them by written agreement to maintain confidentiality and security obligations consistent with Brivo's own.

(C) Duration of agreement and data disposition upon expiration

The subscription is annual and renews each school year. Summit may export cardholder and event data at any time. Upon termination, Brivo deletes account data in accordance with its data retention policy, except where retention is required by law.

(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@summitnyack.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 Brivo's cloud environment hosted on Amazon Web Services data centers located in the United States.

(F) Security protections in place

Data is encrypted in transit (TLS) and at rest. Brivo maintains SOC 2 Type II attestation, role-based administrator permissions, multi-factor authentication for administrators, and 24/7 monitoring. Summit limits administrative access to facilities and IT staff and deactivates credentials on separation. Brivo 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.

Staff-only system; no student records. Kept on file. This supplemental information is based on representations made in Brivo'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	Singlewire Software, LLC, 1002 Deming Way, Madison, WI 53717
Contract / Service	InformaCast emergency mass notification for staff (paging, phone, SMS, email, and mobile app alerts)
Data shared	Staff first and last names, email addresses, and phone numbers; distribution list and security-group membership; notification send and receipt records
Population	Staff
Agreement / term	Annual subscription, renewed each school year

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

Data is used solely to deliver emergency and operational notifications to Summit staff and to record notification delivery. Singlewire may use PII only to provide, support, and secure the service and for no other purpose, including marketing.

(B) Subcontractors / further disclosure

Singlewire uses Amazon Web Services for hosting and third-party carriers and gateways for SMS, voice, and email delivery, solely as necessary to deliver notifications, and requires these subprocessors to maintain confidentiality and security obligations consistent with its own.

(C) Duration of agreement and data disposition upon expiration

The subscription is annual and renews each school year. Contact data is synchronized from Summit's directory and can be removed by Summit at any time. Upon termination, Singlewire deletes customer data in accordance with its retention policy.

(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@summitnyack.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 Singlewire's InformaCast cloud environment hosted on Amazon Web Services in the United States; encrypted backups are stored in AWS.

(F) Security protections in place

Data is encrypted in transit (TLS) between the mobile app, on-premises components, and the InformaCast cloud. SMS messages and email are delivered over carrier networks and are not encrypted

end-to-end, so Summit does not include student information in notification content. Server backups are encrypted with customer-supplied keys. Access is restricted through role-based administrator permissions and multi-factor authentication. Singlewire 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.

Staff-only system; no student records. Kept on file. This supplemental information is based on representations made in Singlewire'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	CENTEGIX, LLC, Atlanta, Georgia
Contract / Service	CENTEGIX CrisisAlert — wearable staff alert badges, incident alerting, and campus safety platform
Data shared	Staff names, roles, badge assignments, and location during alerts; incident records, which may reference a student's name when an alert concerns a specific student
Population	Staff; students only as referenced in incident records
Agreement / term	Annual subscription, renewed each school year; Data Privacy Agreement on file

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

Data is used solely to operate Summit's staff alert and incident response system: issuing and locating alerts, notifying responders, and maintaining incident records. CENTEGIX may use PII only to provide, support, and secure the service and for no other purpose, including marketing.

(B) Subcontractors / further disclosure

CENTEGIX uses cloud hosting (Amazon Web Services) and notification subcontractors solely as necessary to deliver the service and requires them by written agreement to maintain confidentiality and security obligations consistent with its own.

(C) Duration of agreement and data disposition upon expiration

The subscription is annual and renews each school year. Upon termination, CENTEGIX deletes customer data within the period specified in the Data Privacy Agreement, except where retention is required by law, and confirms destruction on request.

(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@summitnyack.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 CENTEGIX's cloud environment hosted on Amazon Web Services data centers located in the United States.

(F) Security protections in place

Data is encrypted in transit (TLS) and at rest (AES-256). Access is restricted through role-based administrator permissions and multi-factor authentication. CENTEGIX maintains SOC 2 Type II attestation and an incident response program. Summit instructs staff to record student names in incident records only when necessary. CENTEGIX 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 CENTEGIX'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@summitnyack.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.

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	monday.com Ltd., Tel Aviv, Israel, with U.S. offices in New York, NY
Contract / Service	monday.com work management — IT help desk and facilities request tracking for staff
Data shared	Staff names and email addresses (requesters and assignees) and the content of service requests. Student information is not stored; staff are instructed not to enter student names or details in requests.
Population	Staff
Agreement / term	Annual subscription, renewed each school year

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

Data is used solely to receive, track, and resolve IT and facilities service requests submitted by Summit staff. monday.com may use PII only to provide, support, and secure the service and for no other purpose, including marketing or training of models on Summit content.

(B) Subcontractors / further disclosure

monday.com engages subprocessors, including its cloud hosting provider (Amazon Web Services), solely as necessary to deliver the service, and requires them by written agreement to protect customer data consistent with monday.com's DPA. monday.com publishes its subprocessor list and provides notice of changes.

(C) Duration of agreement and data disposition upon expiration

The subscription is annual and renews each school year. Summit may export boards at any time. Upon termination, monday.com deletes customer data within the period specified in its DPA, 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@summitnyack.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 on Amazon Web Services data centers in the United States region selected for Summit's account.

(F) Security protections in place

Data is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256). monday.com maintains SOC 2 Type II and ISO/IEC 27001, 27017, and 27018 certifications, supports single sign-on and two-factor authentication, and provides role-based permissions and audit logs. Summit restricts board access to IT and facilities staff. monday.com 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.

Staff-only system; no student records. Kept on file. This supplemental information is based on representations made in monday.com's Data Security and Privacy Plan, contract, and published security documentation, and is reviewed annually by Summit's Data Protection Officer.