Data Privacy and Security Policy

Adopted: September 2026 | Last reviewed: September 2026 | Policy owner: Data Protection Officer

Aligned to NY Education Law § 2-d and 8 NYCRR Part 121.

1. Purpose

Summit School / Summit Children's Residence Center ("Summit," "we," "our") collects and maintains personally identifiable information about the students we serve, their families, and our staff in order to provide educational, residential, and related services. This policy explains what information we collect, how we protect it, who we share it with, and the rights of parents, students, and staff regarding that information.

Summit is an approved private school for the education of students with disabilities and is therefore an "educational agency" under New York Education Law § 2-d and Part 121 of the Regulations of the Commissioner of Education. This policy, our Parents' Bill of Rights for Data Privacy and Security, and supplemental information for each third-party contractor that receives personally identifiable information are published on our website at www.summitnyack.com/data-privacy.

2. Scope

This policy applies to all Summit officers, employees, contractors, volunteers, and third-party contractors who collect, access, store, transmit, or otherwise handle:

- **Student data** — personally identifiable information (PII) contained in student records maintained by Summit, including education, IEP, residential, health, and behavioral records, as defined under FERPA (34 CFR § 99.3) and Education Law § 2-d.
- **Family data** — PII about parents, guardians, and household members collected in connection with a student's enrollment or care.
- **Staff data** — PII about employees and applicants, including "private information" as defined by the New York SHIELD Act (General Business Law § 899-aa), such as Social Security numbers, financial account numbers, and driver's license numbers.
- **Website visitor data** — information collected through our public website and online forms (see Section 12).

3. Legal framework

Summit protects personal information in accordance with the following laws and standards, as applicable:

- New York Education Law § 2-d and 8 NYCRR Part 121 (student, teacher, and principal data privacy and security).
- The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99.
- The Individuals with Disabilities Education Act (IDEA) confidentiality provisions, 34 CFR §§ 300.610–300.627.
- The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506, where online services are used with students under 13.
- The Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h.

- The New York SHIELD Act, General Business Law §§ 899-aa and 899-bb (breach notification and reasonable safeguards for private information of New York residents, including staff).
- The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), adopted by NYSED under 8 NYCRR § 121.5 as the standard for data security and privacy.

Where a placing school district's own Education Law § 2-d policy or contract imposes additional requirements on Summit as a recipient of that district's student data, Summit complies with those requirements as well.

4. Definitions

Personally identifiable information (PII)	For students, PII as defined in FERPA (34 CFR § 99.3): the student's name; the names of parents or family members; the address; personal identifiers such as a student ID or Social Security number; indirect identifiers such as date or place of birth; and any other information that alone or in combination is linkable to a specific student with reasonable certainty. For staff, "private information" as defined by GBL § 899-aa.
Student data	PII from the student records maintained by Summit.
Teacher or principal data	PII from records relating to annual professional performance reviews (APPR), to the extent Summit maintains any such records.
Third-party contractor	Any person or entity, other than Summit, its employees, or a placing school district, that receives student data or teacher/principal data from Summit under a contract or written agreement in order to provide services to Summit (for example, student information systems, learning platforms, cloud productivity suites, communication tools, and data hosting).
Breach or unauthorized release	The unauthorized acquisition, access, use, or disclosure of student data or teacher/principal data by or to a person not authorized to acquire, access, use, or receive it.
Data Protection Officer (DPO)	The person designated by Summit under 8 NYCRR § 121.8 (which may be an employee or a qualified outside consultant) to implement this policy and serve as the point of contact for data privacy and security.
Encryption	Methods of rendering PII unusable, unreadable, or indecipherable to unauthorized persons, consistent with 8 NYCRR § 121.1 and NIST standards.

5. Data Protection Officer

Summit has designated the following Data Protection Officer, who is responsible for implementing this policy, coordinating compliance with Education Law § 2-d and Part 121, responding to complaints, overseeing third-party contractor agreements, and coordinating breach response:

Name / Title	Jeremy Schwarz, President / CEO, S5 IT Consulting, LLC (Data Protection Officer for Summit)
Mailing address	Summit School / Summit Children's Residence Center, 339 North Broadway, Upper Nyack, NY 10960
Email	privacy@summitnyack.com (shared mailbox monitored by the DPO, the Director, and IT); direct: Jeremy@s5itc.com
Phone	(862) 412-8321

6. Privacy principles

In handling PII, Summit will:

- Collect only the PII that is necessary to provide educational, residential, health, and related services and to meet legal and reporting obligations (data minimization).
- Use PII only for the purposes for which it was collected, and disclose it only as permitted by FERPA, IDEA, and Education Law § 2-d.
- **Never sell** student data or teacher/principal data, and never use or disclose it for marketing or commercial purposes, or permit a third-party contractor to do so.
- Not release student data for commercial purposes, and not disclose it to a third party except as authorized by law and, where required, with parental consent.
- Maintain a written inventory of the student data elements we collect and the systems and contractors that hold them.
- Give parents and eligible students the rights described in the Parents' Bill of Rights, including the right to inspect and review records and to challenge the accuracy of PII.
- Apply this policy to PII in every form — electronic, paper, and verbal.

7. Third-party contractors

7.1 Before sharing PII

Summit will not disclose student data or teacher/principal data to a third-party contractor unless a written contract or Data Privacy Agreement is in place that meets Education Law § 2-d(5) and 8 NYCRR § 121.6. The contract must include:

- The Summit Parents' Bill of Rights for Data Privacy and Security.
- A statement of the exclusive purposes for which the data will be used.
- The contractor's **Data Security and Privacy Plan** describing how it will (a) implement all applicable state, federal, and local privacy requirements and Summit's policies; (b) maintain administrative, operational, and technical safeguards aligned with the NIST Cybersecurity Framework; (c) demonstrate compliance; (d) train its employees who have access to PII; (e) bind subcontractors to the same requirements; (f) manage data security and privacy incidents, including prompt notification to Summit; and (g) return, delete, or destroy PII when the contract ends.
- A commitment to encrypt PII in transit and at rest.

- A prohibition on selling PII, using it for marketing or commercial purposes, or disclosing it to any other party without Summit's authorization or as required by law.
- An obligation to notify Summit of any breach or unauthorized release within **seven (7) calendar days** of discovery, and to cooperate with Summit's investigation and any required notifications.
- The contract term, and what happens to PII at expiration or termination.

7.2 Supplemental information published on our website

For every contract with a third-party contractor that receives PII, Summit publishes the supplemental information required by 8 NYCRR § 121.3(c) on the same web page as this policy: the exclusive purposes for which the data is used; how the contractor ensures subcontractors comply; the contract term and disposition of data at expiration; how a parent, student, or staff member may challenge the accuracy of data; where the data is stored and the security protections in place; and how the data is encrypted in transit and at rest.

7.3 Contractor obligations

Each third-party contractor must, in accordance with 8 NYCRR § 121.9: adopt technologies, safeguards, and practices that align with the NIST CSF; comply with this policy and Education Law § 2-d; limit internal access to PII to those employees with a legitimate educational interest; not use PII for any purpose other than those explicitly authorized in the contract; not disclose PII to any other party without prior written consent of the parent or eligible student (or as required by law); maintain reasonable administrative, technical, and physical safeguards; use encryption to protect PII in motion and at rest; and not sell PII or use or disclose it for marketing purposes.

7.4 Vendor review

The DPO, in coordination with the IT department, reviews proposed software and services before adoption to determine whether PII will be shared, what data elements are involved, whether the vendor will sign Summit's Data Privacy Agreement (or an equivalent NY Education Law § 2-d rider), and whether the vendor's security posture is acceptable. Staff may not enter into "click-through" agreements or use free or trial online services with student PII without DPO approval.

7.5 Artificial intelligence tools

Generative AI and other AI-enabled tools (chatbots, writing assistants, transcription, image generation, and AI features embedded in other software) are third-party contractors when they receive PII, and the requirements of this Section apply to them in full. In addition:

- No student, family, or staff PII may be entered into any AI tool unless the specific tool has been approved by the DPO and is covered by a signed Data Privacy Agreement under a commercial or enterprise agreement that prohibits training on Summit data. Free, trial, or personal AI accounts are never approved for PII.
- Even with an approved tool, staff use de-identified data (identification numbers or codes in place of names, and no more detail than the task requires) whenever the task does not require identifying a student. IEPs, evaluations, and health or behavioral records are not processed by AI tools without the DPO's written approval.
- AI features built into approved systems (for example, AI assistants in productivity suites or databases) are disabled for bases, folders, or accounts containing student PII unless the vendor's Data Privacy Agreement covers the AI feature.

- Meetings, IEP conferences, and clinical sessions are not recorded or transcribed with AI tools without approval and required consents.
- Summit publishes the AI tools approved for use with PII on its Data Privacy web page; any tool not listed is not approved.
- Staff remain responsible for the accuracy and appropriateness of any work product created with AI assistance, and students may use AI tools only as directed by their teachers and the Student Acceptable Use Policy.

8. Data security standards

Summit adopts the NIST Cybersecurity Framework as the standard for its data security and privacy program, consistent with 8 NYCRR § 121.5. Safeguards include:

- **Identity and access** — centralized identity management; unique user accounts; role-based access limited to a legitimate educational or business need; multi-factor authentication for staff accounts and administrative access; prompt de-provisioning when staff leave or change roles.
- **Encryption** — PII is encrypted in transit (TLS 1.2 or higher) and at rest in the systems that store it; full-disk encryption on Summit-managed laptops and mobile devices.
- **Endpoint and network protection** — managed devices with current operating system and security updates; endpoint protection; segmented networks; firewall and content filtering; secure Wi-Fi.
- **Monitoring and logging** — audit logs for systems containing PII; review of access and security alerts.
- **Physical safeguards** — locked storage for paper records; controlled access to server and network equipment; secure disposal of paper and media.
- **Backup and recovery** — regular backups of critical systems, stored securely and tested for restoration.
- **Least-privilege data sharing** — PII is transmitted to placing districts, agencies, and contractors only through secure, approved channels (encrypted file transfer, secure portals, or encrypted email); PII is not sent to personal accounts or unmanaged devices.
- **Periodic assessment** — Summit periodically reviews its security controls, policies, and third-party contractor compliance against the NIST CSF.

9. Staff responsibilities and training

All Summit officers and employees with access to PII must:

- Complete annual data privacy and security awareness training as required by 8 NYCRR § 121.7, and acknowledge this policy.
- Access and use PII only as needed to perform their job duties.
- Use only Summit-approved systems and accounts for storing or sharing PII.
- Protect credentials, lock unattended devices, and follow Summit's acceptable use and password requirements.
- Report any suspected breach, unauthorized release, lost device, or phishing incident to the DPO or IT department **immediately**.

Violation of this policy may result in disciplinary action up to and including termination, and may carry civil or criminal penalties under Education Law § 2-d.

10. Breach and unauthorized release

Summit maintains an incident response procedure for actual or suspected breaches or unauthorized releases of PII. In accordance with 8 NYCRR § 121.10:

1. Third-party contractors must notify Summit of any breach or unauthorized release of PII within **7 calendar days** of discovery.
2. Summit will notify the NYSED Chief Privacy Officer within **10 calendar days** of receiving a contractor's notification or of discovering a breach in its own systems.
3. Summit will notify affected parents, eligible students, and staff, and the placing school district where applicable, in the most expedient way possible and without unreasonable delay, and in no case later than **60 calendar days** after discovery (or after notification by a contractor), unless law enforcement requests a delay.
4. Notifications will be in plain language and will describe what happened, what information was involved, the steps Summit has taken, and contact information for further inquiries.
5. For staff "private information" covered by the SHIELD Act, Summit will also make the notifications required by GBL § 899-aa, including to the New York Attorney General, Department of State, and Division of State Police where applicable.

Summit will document each incident, its investigation, and remediation, and may seek reimbursement from a third-party contractor for the cost of notifications resulting from the contractor's breach.

11. Complaints

Parents, eligible students, staff, and other stakeholders may file a complaint about a possible breach or improper disclosure of PII, or about Summit's or a contractor's handling of PII, with the Data Protection Officer using the contact information in Section 5, in writing (mail or email) or by phone. Complaint forms are available from the main office and at www.summitnyack.com/data-privacy.

Summit will acknowledge receipt of a complaint promptly, investigate, and provide the complainant with written findings within **60 calendar days** of receipt. If more time is needed, Summit will notify the complainant in writing of the reason for the delay and the expected completion date. Complaints may also be filed directly with the NYSED Chief Privacy Officer at privacy@nysed.gov or New York State Education Department, Chief Privacy Officer, 89 Washington Avenue, Albany, NY 12234.

12. Website and online services

Our public website (www.summitnyack.com) may be visited without providing personal information. When you submit a form on our site (for example, an inquiry, application, referral, or employment application), we collect only the information you provide and use it solely to respond to your request. Our website may use cookies and analytics tools (Google Analytics) that collect non-identifying usage data; you may disable cookies in your browser. Our website does not knowingly collect personal information from children under 13 without parental consent. Links to third-party sites are subject to those sites' own privacy policies.

Online services used for instruction, communication, and school operations that receive student PII are listed, with their supplemental information, on our Data Privacy web page.

13. Records retention and destruction

Summit retains student records for the periods required by state and federal law and the placing school district's requirements, and securely destroys PII when it is no longer needed. Electronic media are wiped or destroyed and paper records are shredded. Third-party contractors must return or securely delete all Summit PII at the end of their contract and certify destruction upon request.

14. Policy review

The DPO will review this policy at least annually and whenever there is a material change in law, regulation, or Summit's systems, and will update the published third-party contractor supplemental information whenever a contract is added, renewed, or terminated.

15. Related documents

- Parents' Bill of Rights for Data Privacy and Security (published on our website).
- Third-Party Contractor Supplemental Information (published on our website).
- Third-Party Contractor Data Privacy Agreement (template).
- Technology Acceptable Use Policy — Staff; Technology Acceptable Use Policy — Students; FERPA Annual Notice; Data Privacy Complaint Form; Incident Response Procedure; Records Retention Schedule.