

Technology Acceptable Use Policy — Staff

Summit School / Summit Children's Residence Center | Adopted: September 2026 | Applies to all employees, contractors, consultants, and volunteers

1. Purpose and scope

Summit provides computers, networks, accounts, software, and internet access ("Summit technology") to support the education, care, and safety of our students and the operation of the school and residence. This policy sets the rules for using Summit technology and for handling the personal information of students, families, and staff on any device or service. It applies to all Summit technology, to personal devices used for Summit work, and to any online service used with Summit data, on or off campus.

2. General principles

- Summit technology is provided for Summit purposes. Limited, incidental personal use is permitted if it does not interfere with work, violate this policy, or create cost or risk for Summit.
- Use of Summit technology is a privilege that may be limited or revoked. Summit systems, accounts, email, and files are Summit property and may be monitored, accessed, and reviewed by Summit at any time for security, compliance, operational, or legal reasons. **Users should have no expectation of privacy** in anything created, stored, sent, or received on Summit systems.
- Everything you do with Summit technology should be consistent with Summit's mission, professional standards, and the law.

3. Accounts and passwords

- Use only the accounts issued to you. Never share your password or let another person use your account; never use another person's account.
- Use multi-factor authentication wherever Summit enables it. Do not approve MFA prompts you did not initiate — report them to IT.
- Use unique passwords for Summit accounts (not reused from personal accounts). Change your password immediately if you suspect it has been exposed.
- Lock your screen when you step away. Log out of shared computers.
- Accounts are disabled on separation from Summit. Do not attempt to access Summit systems after your employment or engagement ends.

4. Protecting student, family, and staff information

Personally identifiable information (PII) about students, families, and staff is protected by FERPA, IDEA, New York Education Law § 2-d, and the NY SHIELD Act. Staff who handle PII must:

- Access PII only when needed to do your job, and only the minimum needed.
- **Store and share PII only in Summit-approved systems** — currently PowerSchool, Google Workspace (Summit domain), Microsoft 365 (staff only), Orah, and the other systems listed on

Summit's Data Privacy page. Never store PII in a personal email account, personal cloud storage (personal Google Drive, iCloud, Dropbox), personal messaging apps, or on personal devices.

- **Do not enter student or staff PII into any online service, app, website, or AI tool that Summit has not approved and contracted.** This includes free or trial versions of software, "sign up with Google" apps, and personal ChatGPT, Claude, Gemini, or similar accounts. Approved tools are listed on the Data Privacy page; ask the Data Protection Officer or IT before using anything else.
- Send PII to placing districts, agencies, or families only through approved channels: encrypted email, secure portals, or secure file transfer. Do not send IEPs, evaluations, or health information by unencrypted email or text message. Double-check recipients before sending.
- Do not text or message about identifiable students on personal phones or personal messaging apps. Use Summit systems.
- Keep paper records with PII in locked storage; do not leave them on desks, in vehicles, or at printers. Shred when no longer needed.
- Do not photograph, record, or post images or video of students except as authorized by your role and the student's signed media release, and never on personal social media.
- Do not discuss identifiable student information in public areas or where it can be overheard by people without a need to know.
- If you leave Summit, you may not take PII with you in any form.

5. Devices

- Summit-issued laptops, phones, and tablets must remain enrolled in Summit device management, encrypted, and kept up to date. Do not disable security software, remove management, or "jailbreak" devices.
- Personal devices may be used for Summit email or approved apps only if enrolled in Summit's mobile management or otherwise approved by IT, and must have a passcode and current updates. Summit may remove Summit data from a personal device on separation or loss.
- Report a lost or stolen device to IT **immediately**, on the same day.
- Do not connect unknown USB drives or unapproved hardware to Summit networks or devices.

6. Email, internet, and communications

- Use your Summit email for Summit business. Be professional — email is a record and may be disclosed in legal proceedings.
- Be alert to phishing. Do not click links or open attachments in unexpected messages, and do not enter your Summit password on a page reached from an email link. Report suspicious messages to IT.
- Do not use Summit technology to access, store, or send content that is illegal, harassing, discriminatory, sexually explicit, or otherwise inconsistent with Summit's mission, or to conduct outside business.
- Do not attempt to bypass content filtering, access systems or data you are not authorized to use, or install unapproved software.
- Communications with students and families must be through Summit-approved channels and consistent with Summit's staff-student boundary expectations. Do not "friend," follow, or message students on personal social media.

7. Artificial intelligence tools

- AI tools (chatbots, writing assistants, transcription, image generators) may be used for Summit work only if the specific tool is approved by the Data Protection Officer and listed on the Data Privacy page, or if no student, family, or staff PII is involved in any form.
- Even with an approved tool, use de-identified information (no names, IDs, or details that identify a student) whenever the task does not require identification.
- Do not record or transcribe meetings, IEP conferences, or clinical sessions with AI tools without approval and the required consents.
- Staff remain responsible for the accuracy and appropriateness of anything produced with AI assistance.

8. Reporting incidents

Report any of the following to the IT department and the Data Protection Officer (privacy@summitnyack.com) **immediately**: a lost or stolen device; a suspected phishing compromise or shared password; PII sent to the wrong recipient; PII found in an unapproved system; a vendor or website behaving suspiciously; or any suspected unauthorized access to Summit systems. Prompt reporting is required by law and is never treated as a disciplinary matter in itself; failure to report is.

9. Training

All staff complete data privacy and security training on hire and annually thereafter, and acknowledge this policy each year.

10. Consequences

Violations of this policy may result in loss of technology privileges, disciplinary action up to and including termination, and referral to law enforcement. Unauthorized disclosure of student data may also carry civil penalties under Education Law § 2-d.

Staff acknowledgment

I have read and understand the Summit Technology Acceptable Use Policy — Staff and the Summit Data Privacy and Security Policy. I understand that Summit technology and accounts may be monitored, that I must handle student, family, and staff personal information only as described above, and that violations may result in discipline.

Name (print)	
Position / department	
Signature	
Date	