VENDOR SUBMISSION / REVIEW DRAFT

District vendor & data governance packet

Prepared for Dr. McKinley and Ms. Lena Alonso
Gwinnett County Public Schools • Submitted by Aliasgar Baldiwala

Purpose

Support the district’s third-party vendor and student-data review of Rooftop Crew, an after-school attendance and campus pickup tracker. This packet is an overview for review—not a signed data agreement, district endorsement, legal opinion, or authorization to use student records.

Product scope

Staff import a roster, print QR badges, record check-ins and check-outs, and review campus pickup locations and student timelines. Guardians see linked children and choose alert preferences. Administrators manage access and may use an operational AI assistant.

What is included

Pages 1–6: current data-handling summary, controls, limitations, and requested review decisions. Appendix: the existing 11-slide governance presentation (11 landscape pages). The clarifications on summary page 6 qualify broader claims in that presentation.

Review access

Website: https://afterschool.nasrllc.com
Use fictional demo data for committee walkthroughs. Arrange individual review access privately; this packet contains no login credentials or student records.

Recommended review position: do not introduce additional live student records until the district authorizes the data source, access arrangements, processing terms, and retention policy.

DATA INVENTORY

What the app handles

Records support attendance, pickup coordination, account access, and operational summaries.

Students & guardian contact details

Student code/unique ID; first and last name; grade; optional photo URL; guardian name, email, and phone; email/text alert preferences. A student code is an identifier, not anonymous data.

Attendance & campus locations

Check-in/check-out records contain student and location IDs, action, timestamp, optional note, and recording user ID. Pickup locations contain names, map coordinates, directions, and accessibility notes. Locations describe campus pickup points, not continuous GPS tracking of a child.

Accounts, audit & messaging

Account profiles and assigned roles; student-page access log entries; notification records with channel, recipient, message, status, and creation time; stored assistant user/response messages. The audit log records individual student-history access, not every possible student-data read.

Where processing occurs

The app uses Lovable Cloud for accounts and application records. Staff devices hold pending offline scans. The optional administrator assistant sends a reduced attendance snapshot and conversation text through Lovable AI Gateway to the configured OpenAI model. Provider processing locations, subprocessors, and contractual safeguards require confirmation.

Data minimization before a pilot: confirm which fields the district permits; omit unnecessary photos, contact details, and free-text notes. Do not put sensitive health, disability, disciplinary, or family details in notes or AI questions.

ACCESS & ACCOUNTABILITY

Who can do what

School-controlled roles and guardian-scoped records are intended to limit exposure.

Administrators & staff

New non-parent accounts wait for administrator approval before receiving a role. Administrators approve or remove staff access and manage privileged settings. Approved staff record attendance and access authorized student records. The AI endpoint separately checks administrator access.

Guardians

Guardian visibility is based on the signed-in email matching the guardian email on the student record. Parent-intent signup alone does not link a child. Guardians may update their linked child’s alert preferences; a database-level guard blocks changes to student identity and other protected fields.

Record integrity & viewing logs

Check-in/out records are add-only through the app. Individual student-history access attempts a viewing-log entry with viewer, student, and time; administrators can review the log. The current log does not cover every roster, dashboard, parent-summary, or assistant read, and is not a comprehensive access audit.

District review actions

Confirm guardian linkage and email-verification requirements; identify authorized approvers; review staff access periodically; define correction and revocation procedures; and agree any additional audit coverage needed. Reviewers should not assume sign-out, account removal, and device cleanup are equivalent.

Evidence status: these controls were implemented and selected approval/guardian scenarios were tested earlier. This packet includes a source review, not a fresh authenticated test of every control or a new security assessment.

EXTERNAL PROCESSING & HANDHELDS

AI and offline-device handling

Reduced identifiers lower exposure, but do not make attendance data anonymous.

What the assistant receives

The attendance snapshot uses student codes in place of roster names and includes grade, attendance status, campus location names, times, and movement history. Conversation text is masked with roster-name substitution before model submission. Guardian contact fields are not included in the structured snapshot.

Limits of name masking

Masking is best-effort text substitution: a partial, differently formatted, or manually entered name or other identifier may remain. Original user message parts are saved in the app before masking. Do not enter names, contact details, or sensitive information in questions. “The AI never sees a name” is not an absolute guarantee.

Provider terms still need review

The configured model is OpenAI GPT-6 Astra through Lovable AI Gateway. Requests specify store=false; that setting alone does not establish all provider retention, training, residency, or deletion commitments. Obtain applicable processing terms and district approval before real-record AI use. AI summaries must be checked against attendance records, not relied on alone for child safety decisions.

Offline scans on staff devices

The browser’s pending queue includes student IDs, names and codes, location IDs/names, action, timestamp, and queue ID. Successfully replayed scans are removed; failed entries remain. This queue is not codes-only. Use school-managed devices and establish lock, lost-device response, queue cleanup, and shared-device procedures before deployment.

RETENTION & SERVICE READINESS

Current settings, not policy approval

Documented retention intervals are provisional and require district confirmation.

Scheduled record retention

A nightly purge is documented for check-in/out records and notification records older than one year; assistant conversations older than 90 days; and student-access logs older than two years. These intervals were implementation defaults, not district-selected policy. Current scheduler execution and purge results were not revalidated for this packet.

Items without an established lifecycle here

The listed purge does not establish deletion periods for student rosters, guardian contacts, accounts, photos, printed badges, offline device data, or backups. Agree archival/export, student withdrawal, contract-end deletion, legal holds, backup expiry, and deletion evidence separately.

Email & text delivery are not ready

Alert preferences and notification records exist. School email setup and actual email delivery remain unconfirmed. SMS requires a separately configured sending service and consent workflow; connecting an email domain does not enable text delivery. Daily email delivery and a delivery-history page are not complete.

Security & operational evidence to request

Obtain a dated assessment, current access-policy tests, provider security documentation, incident reporting contacts and timeline, recovery objectives, backup/restore evidence, and operating responsibilities. Past platform scans are not independent penetration testing, ongoing assurance, or FERPA certification. Encryption and hosting-residency claims must be supported by provider documentation.

DISTRICT DECISIONS & APPENDIX NOTES

Before a live-data pilot

Request the district’s official vendor process and data-governance requirements; this is not its required form.

Requested next steps

1. Confirm the appropriate vendor registration portal, contact, and required documents.
2. Identify the submitting legal entity; provide W-9, insurance, and procurement details if requested.
3. Review a district-approved data processing agreement, permitted purpose, role of service providers, and any FERPA school-official requirements with district counsel.
4. Approve data fields, roster source, guardian linkage, access administration, and AI use.
5. Set retention/deletion and incident-response requirements, then validate controls with fictional data before authorizing a limited live-data pilot.

Clarifications that qualify the appended deck

Audit (slides 2, 9–10): logging covers the individual student-history flow, not every view or read.
AI (slides 6, 8, 10–11): the snapshot contains codes plus attendance context; free-text masking is best effort, not guaranteed anonymization.
Security (slides 7, 10): earlier platform scan results are historical, not independent certification or a fresh assessment.
Messaging (slides 5, 11): email and SMS each need delivery setup and validation; email-domain setup alone is insufficient.
Performance (slide 4): “under two seconds” is descriptive, not a measured service guarantee.

Submission boundaries

The following presentation is retained as background product material. This summary is the current qualification of its claims. No W-9, insurance certificate, signed agreement, certification, or district approval is represented as obtained or attached. No credentials, live student data, or source-code deposit are included.

Basis: existing governance presentation and documented implemented controls, plus an October 21, 2026 source review of student data access, offline scans, guardian views, and assistant processing. Deployed configuration and vendor contractual terms remain subject to verification.

ROOFTOP CREW

After-School Tracker

Every student accounted for, from last bell to pickup.

Built for Gwinnett County after-school programs — with child data governance built in.

The problem

Unscheduled after-school events leave nobody knowing where a child is

Today

A club runs late, practice moves fields, a bus is delayed — and no one can say where a student is. Parents call the front office. Staff radio each other. The child is fine, but nobody can prove it.

What families expect

During school hours, every student is tracked. After school should be no different: one scan at check-in, one at pickup, and a parent who always knows.

The stakes

These are children, and their records are sensitive. Any system that tracks them must control who sees what, log every view, and keep data only as long as needed — that is built in, not bolted on.

How it works

Three steps, designed for a handheld device

1. Roster

Students are uploaded once with a unique ID — by CSV import or one at a time. Each student gets a printable QR badge.

2. Scan

Staff scan a badge at any pickup spot to check a student in or out. Works offline — scans queue on the device and sync when signal returns, keeping the original time.

3. Locate

Admins see every student's status on a live dashboard and campus map. Parents see their own child's pickup spot, directions, and timeline.

Built for staff on the move

Fast scanning, real places, no signal required

QR scanning

Point the camera at a badge — check-in or check-out in under two seconds. Bulk badge printing for the whole roster.

Campus map

Real pickup locations pinned on the school map, with directions and accessibility notes. Admins can edit pins as spots change.

Offline-first

Dead signal at the field? Scans save on the device with the true timestamp and sync automatically when the device reconnects.

Evening timeline

A live list of who is still on campus, longest-waiting first, with last check-in time and location — so no child is left unaccounted for.

What parents see

Their own children — and nothing else

Self sign-up

Guardians create their own account. When their email matches the guardian email on a student's record, the link is automatic — no admin data entry.

Live status

Check-in status, today's pickup spot with directions and accessibility notes, and a full timeline of every scan with map links.

Alert opt-in

Parents choose email or text alerts per child for check-ins and check-outs. (Sending goes live once the school email domain is connected.)

Admin dashboard & AI assistant

Answers without digging through records

Live dashboard

Any student's status and location at a glance. Staff access approvals, role management, and a full access log — all in one place.

AI ops assistant

Ask plain questions — "who is still on campus?" — and get a concise operational summary. Privacy-protected: the model only ever sees student codes, never names.

Demo mode

A full sample afternoon with 12 made-up students for presentations and training. Demo scans never touch real records, and real settings can't be changed while demo mode is on.

Data governance — built for child data

Designed for district review and FERPA-aligned handling

Least privilege

New accounts get no access until an admin approves them. Parents are matched only by guardian email. No one can grant themselves a role — self-promotion is refused at the database level.

Scoped views

Parents see only their own linked children. Staff and admin roles are separate and admin-granted. Check-in records are add-only — they cannot be edited or deleted through the app.

Verified clean

Independent security scan of the database: no open findings. Every table is protected by row-level rules enforced by the database itself, not just the app.

Guardian rights & AI privacy

Two protections worth calling out

Guardians can only change alert preferences

A parent can toggle email/text alerts for their child — and nothing else. Name, ID, pickup location, and the guardian email on file are locked to staff. This is enforced by a database trigger, so it holds no matter what the app does. A parent cannot reassign their child's record to another account.

The AI never sees a child's name

Before any question goes to the AI model, student names are replaced with codes. The model reasons over codes and codes only; the app maps codes back to names on the staff member's own device. Guardian emails and phone numbers are never sent. Child identities stay inside the system.

Audit trail & data retention

Who saw what, and nothing kept forever

Access log

Every time someone opens a student's page, the view is recorded: who, which student, and when. Admins can review the log in the dashboard — full accountability for every pair of eyes on a child's record.

Automatic retention limits

A nightly job purges old records automatically:

- Check-in/out records — 1 year
- Notifications — 1 year
- AI assistant conversations — 90 days
- Access log — 2 years

Retention periods can be adjusted to match district policy.

Governance at a glance

What the committee can verify

Control	How it works	Where enforced
Access approval	No role until an admin approves the account	Database + app
Parent scope	Own linked children only, matched by guardian email	Database rules
Guardian edits	Alert switches only; all other fields refused	Database trigger
AI privacy	Student codes only — no names, emails, or phones	Server, before sending
Audit	Every student page view logged with viewer and time	Database table
Retention	Nightly automatic purge (1 yr / 90 days / 2 yrs)	Scheduled job
Security scan	Independent scan — zero open findings	Platform scanner

Next steps

What we need from the district

Before go-live

Connect the school email domain and sending service so parent alerts and the evening pickup email can actually send. Until then, notifications are recorded but not delivered.

District review

Confirm the retention periods match district policy, approve the roster data source, and review the data agreement for the AI assistant (codes only, no identifiers).

Pilot

Run a pilot with one after-school program using real badges and the campus map. Demo mode is available for every committee meeting and training session.