Rooftop Crew — Information Security Program & Incident Response Plan

NASR LLC · Version 1.0 · October 29, 2026 · Review draft for district vendor review. Not legal advice or a compliance certification.

1. Purpose and scope

- Written security program covering student and guardian data processed by the Rooftop Crew After-School Tracker, prepared to meet COPPA (16 CFR 312.8, as amended 2025), FERPA school-official obligations, and the Georgia Student Data Privacy, Accessibility, and Transparency Act (O.C.G.A. 20-2-660 et seq.).
- Owner: Aliasgar Baldiwala, Founder & CTO (security coordinator). Reviewed at least annually and after any incident.

2. Data we hold

- Student code, name, grade, optional photo; guardian name, email, phone, alert preferences; check-in/out times and locations; staff/parent accounts; record-view log; family privacy requests.
- No Social Security numbers, health, discipline, or academic records are collected.

3. Safeguards in place

- Role-based access enforced in the database: new staff need administrator approval; guardians see only children linked to their email and may change only alert settings.
- Check-in records are add-only; every student-history view is logged for administrators.
- AI assistant receives student codes rather than names; conversations deleted after 90 days.
- Automated nightly deletion: check-ins/alerts 1 year, view log 2 years.
- Family requests to see, correct, or delete records are tracked in the app; administrators can delete a single child's records or all of a school's student data at contract end.
- Automated security scans run before each release.
- No sale of student data, no targeted advertising, no profiling beyond the service (Georgia Act, COPPA).

4. Risk assessment and testing

- Annual written risk assessment of threats to student data, plus review after major changes.
- Independent penetration testing has not yet been performed; it is planned before a live district pilot.

5. Incident response

- **Detect & report:** anyone who suspects unauthorized access emails info@nasrllc.com; the security coordinator opens an incident log entry the same day.
- **Contain (within 24 hours):** revoke affected accounts, rotate credentials, disable affected features, preserve logs.

- **Assess (within 72 hours):** determine what data, which students and schools, and how it happened.
- **Notify:** notify each affected school promptly and within 72 hours of confirmation, or sooner if the district agreement requires, so the school can notify families. Cooperate with law enforcement and follow Georgia breach-notification law (O.C.G.A. 10-1-912).
- **Recover & review:** fix the cause, confirm the fix, document lessons learned and update this plan within 30 days.

6. Retention and deletion

- At contract end or on the school's written request, the school administrator (or NASR LLC at the school's direction) deletes all of the school's student data using the in-app tool, and NASR LLC confirms deletion in writing.
- Hosting-provider backups age out on the provider's schedule; this is disclosed to districts.

7. Service providers

- Lovable Cloud (hosting/database) and Lovable AI Gateway (optional AI assistant). Providers are used only to deliver the service.

8. Training and accountability

- Everyone with access reviews this plan and student-privacy duties on joining and yearly.
- Signed data-processing agreement with each district governs final terms; it prevails over this plan where stricter.