ROCKET DRONES TRUST CENTER

Data Privacy & Security

Clear, documented privacy and security practices for schools, districts, public agencies, and training organizations evaluating Rocket Drones.

Last updated: August 31, 2026

Document	Data Privacy & Security Overview
Provider	Rocket Drones
Platform	SaaS cloud-based web application
Security Contact	Brandon Turk, brandon@rocketdrones.com, 901.440.2797

Overview

Rocket Drones is a SaaS, cloud-based web application developed using Next.js, TypeScript, PostgreSQL, and Supabase. The platform supports drone and aviation education through learning modules, web simulations, classroom workflows, flight logging, racing tools, and reporting features.

Our security model uses managed infrastructure, encryption, role-based access, least-privilege controls, secure development practices, and clear customer data governance.

Core Privacy Principles

Customer ownership

All customer and student data remains owned and controlled by the school, district, municipality, or organization that provides it. Rocket Drones processes data only as necessary to provide, maintain, support, and secure the contracted services.

Limited collection

The platform is designed to collect only the information needed for account access, classroom administration, course participation, simulation activity, assessments, reporting, and support.

No advertising use

Rocket Drones does not sell, rent, exchange, or monetize customer or student data. Student data is not used for targeted advertising, advertising profiles, or unrelated marketing purposes.

Secure operations

Security controls are applied across the application, database, authentication, hosting, network, and support workflows. Administrative access is limited and privileged credentials are kept server-side.

Security Controls

Application security

- Next.js and TypeScript application architecture
- Secure server-side handling of service-role credentials
- Input validation, React output encoding, and secure API practices
- Dependency review through package lockfiles, automated alerts, and package audit tools

Identity and access

- Individual user accounts; shared accounts are discouraged
- Role-based access controls aligned to job responsibilities
- Least-privilege database permissions and Supabase Row Level Security policies
- Multi-factor authentication support where enabled and supported by configuration

Encryption and infrastructure

- HTTPS/TLS for web and application traffic
- TLS/SSL-encrypted database and API communications
- Provider-managed encryption at rest for database and storage services
- Managed hosting, DNS, certificate, backup, and network-edge controls through infrastructure providers

Monitoring and response

- Authentication, application, database, and hosting logs where configured
- Security patch review on an ongoing basis
- Expedited remediation for critical or actively exploited vulnerabilities
- Customer notification for confirmed data incidents according to contract and law

---

Student Data

Exact data elements depend on the customer configuration and features in use. Rocket Drones documents required, optional, and not-applicable student data elements during privacy reviews.

- Student email for login and account access
- Optional student first and last name
- School, class, course, teacher, and enrollment associations where configured
- Course participation, progress, scores, grades, and application performance data where enabled
- Application metadata such as timestamps, IP addresses, browser details, authentication events, and security logs where needed to operate and protect the service

---

Infrastructure Providers

Rocket Drones uses a limited set of essential technical providers to host, route, secure, and operate the service. These providers are paid for infrastructure services and do not monetize customer or student data.

- **Supabase:** Managed PostgreSQL database, authentication, object storage, automated backups, and backend services.

- **Vercel:** Application hosting and delivery for the Next.js web application.
- **Cloudflare:** Authoritative DNS, traffic routing, TLS certificates, and optional network-edge protections.

Governance

Security framework: Practices are informed by OWASP Secure Coding Practices, the NIST Secure Software Development Framework, NIST Cybersecurity Framework principles, and CIS guidance where applicable. Rocket Drones does not currently hold an independent SOC 2 or ISO 27001 certification.

Patch cycle: Critical or actively exploited vulnerabilities are prioritized as soon as reasonably practicable. High-severity issues are targeted within 14 days, medium-severity issues within 30 days, and lower-severity issues through the normal release cycle.

Data export: Authorized customers may request data export in commonly readable formats such as CSV, JSON, or PostgreSQL-compatible exports, depending on technical feasibility.

Data deletion: Customer data can be deleted from active application systems upon authorized request or contract termination, subject to legal obligations, technical feasibility, and backup-retention schedules.

Breach notification: Rocket Drones provides notice of confirmed data breaches without unreasonable delay and according to applicable contractual obligations.
