



Security & Privacy Overview

This overview is intended for IT, procurement, and compliance staff evaluating FalconEye for school or program use. It summarizes practices described more fully in our Software Subscription Agreement, Data Processing Addendum, and Privacy Policy..

What Data We Handle

Account information (name, email, school/program, role), Customer-uploaded film and scouting statistics, player performance data, and basic usage/log data. We do not knowingly collect data directly from children under 13, and player accounts are provisioned only by school/program staff, never self-registered by students.

Data Ownership and Use

Customers retain ownership of all content they upload. FalconEye does not sell Customer Content, does not use it to train models for unrelated third parties, and does not engage in targeted advertising.

Legal & Regulatory Alignment

- FERPA — FalconEye acts as a “school official” performing an institutional service under the customer’s direct control, consistent with 34 C.F.R. § 99.31(a)(1).
- COPPA — Player accounts are staff-provisioned, not self-registered; customers are responsible for parental consent where required.
- Where a Customer is subject to a state student-data-privacy law, FalconEye supports the Customer’s compliance and does not sell student data or use it for targeted advertising. The specific obligations of each party are governed by the Subscription Agreement and the DPA.
- State consumer privacy laws (e.g., CCPA/CPRA and other comprehensive state privacy laws) — FalconEye does not sell personal information or use it for targeted advertising.

Technical & Organizational Safeguards

- Encryption of data in transit and at rest
- Role-based access controls, configured by each customer for its own staff
- Routine internal security review of the platform
- Backups maintained to support recovery and data export
- Vendor/subprocessor relationships governed by confidentiality and security obligations

Data Retention & Deletion

Customer Content is retained for the duration of an active subscription and for a limited period afterward to allow export, after which it is deleted from active systems except as retained in backups or required by law. Deletion requests can be directed to chris@falconeyefaceoff.com.

Incident Response

FalconEye maintains an internal process for identifying, containing, and investigating security incidents. In the event of a confirmed security incident involving customer data, FalconEye will notify the affected customer without undue delay, and in no event later than five (5) business days after confirmation, so the customer can meet its own notification obligations.

Subprocessors

A current subprocessor list is maintained and available on request. Subprocessors are bound by confidentiality and security obligations no less protective than this policy.

Compliance Roadmap

FalconEye is a growing platform and does not yet hold a formal third-party security certification (e.g., SOC 2). We are happy to complete customer security questionnaires and to discuss our roadmap toward formal certification directly.

Contact

Security and privacy questions: chris@falconeyefaceoff.com