



Privacy Policy

Last modified: September 3rd, 2026

1. Introduction and Scope

This Privacy Policy ("Policy") describes how FalconEye-Faceoff Intelligence System LLC, a Pennsylvania limited liability company with a principal place of business at 502 W 7th St STE 100, Erie, PA 16502 ("FalconEye," "we," "us," or "our"), collects, uses, discloses, and safeguards information in connection with (a) falconeyfaceoff.com and any other website we operate that links to this Policy (the "Website"), and (b) the FalconEye scouting, analytics, and coaching platform, including all associated web applications, APIs, and related services (the "Service").

This Policy applies to:

- Customers (schools, athletic departments, clubs, programs, and independent trainers that subscribe to the Service) and their Authorized Users (coaches, athletic staff, administrators, and student-athletes who access the Service on a Customer's behalf);
- visitors to the Website; and
- individuals who request a demo, start a free trial, or otherwise communicate with us about the Service.

This Policy does not apply to information a Customer processes using its own systems outside the Service, or to third-party websites or services that we do not own or control, even if linked from the Service or the Website.

2. Relationship to the Subscription Agreement and DPA

FalconEye's processing of data that customers and their authorized users upload to the Service ("Customer Data"), including student information, is performed on the customer's behalf and is governed by the FalconEye Software Subscription Agreement and the Data Processing Addendum (the "DPA") between FalconEye and the customer. In the event of any conflict regarding Customer Data, those agreements control.

3. Information We Collect

3.1 Account and Registration Information.

When a Customer Admin provisions an account, or an Authorized User registers or logs in, we collect information such as name, email address, school or program affiliation, role (for example, head coach, assistant coach, athletic administrator, or student-athlete), and login credentials. If you sign in using a third-party single sign-on option such as Google, we receive the name, email address, and basic profile information that your Google account authorizes us to receive. We do not receive your Google password.

3.2 Customer Data, Including Student Data.

Customers and their Authorized Users upload, input, or generate Customer Data within the Service. This may include video footage of faceoffs, draws, and other game or practice film; scouting notes; player statistics, tendencies, jersey numbers, positions, and similar performance information; practice plans; and related film-analysis data. Some Customer Data includes Personal Information about identifiable student-athletes, coaches, or staff, and some may include student information. FalconEye does not collect this information directly from individual student-athletes; Customer determines what Customer Data to submit, and about whom. FalconEye processes Customer Data on the Customer's behalf under the Subscription Agreement and the DPA, which govern the operative terms of that processing.

3.3 AI Customer Input and AI Customer Output.

When Customer or an Authorized User uses an AI Feature of the Service, including film breakdown, scouting analysis, tendency tracking, scoring, ranking, and the Ask FalconEye assistant, the film, text, prompts, images, or other content submitted to that feature ("AI Customer Input") is processed, including by Third-Party AI Technology described in Section 6, to generate analytics, scores, reports, tendency profiles, and other content ("AI Customer Output") for Customer.

3.4 Billing Information.

If Customer purchases a paid subscription, billing-related information (such as billing contact name, institution name, billing address, and payment details) is collected and processed on our behalf by our third-party payment processor, Authorize.Net. FalconEye does not directly receive, process, or store full payment card numbers.

3.5 Usage Data.

We, and our service providers, automatically collect certain information when the Service or Website is accessed, including IP address, browser type and version, operating system, device identifiers, referring and exit pages, the features or pages accessed, timestamps, and similar log, diagnostic, and telemetry data ("Usage Data"). Some Usage Data, such as aggregate traffic, performance, diagnostic, and telemetry data, does not identify Customer or any individual. Other Usage Data is associated with a specific account (for example, administrative dashboards within the Service may display a named Authorized User's login and activity history (such as name, school or program, and timestamps)) and, in that context, may identify an individual. FalconEye uses account-linked Usage Data to operate, secure, support, and administer the Service, including to authenticate users and to monitor for unauthorized access, credential sharing, or misuse.

3.6 Communications and Support.

If you contact us for technical support, sales inquiries, a product demo, or general questions, we collect the information you provide, such as your name, email address, institution, and the content of your message, along with any attachments.

3.7 Cookies, Local Storage, and Similar Technologies.

The Service uses browser cookies, local storage, session storage, and similar technologies to authenticate users, maintain login sessions, remember preferences, and support core application functionality. Where the Service embeds third-party video, for example film clips hosted on YouTube, we use a privacy-enhanced

embed mode that does not set an advertising or tracking cookie unless you choose to play the video. FalconEye does not use the Service to deliver third-party behavioral advertising or cross-site ad tracking.

The Website currently uses Vercel Analytics and Google Search Console to understand website traffic and performance. Neither tool sets an advertising or marketing cookie, and the Website does not otherwise use cookies or similar technologies for advertising or cross-site tracking. If FalconEye adds additional analytics or advertising technologies to the Website in the future, this Policy will be updated accordingly. See Section 18 for information on Do Not Track and Global Privacy Control signals.

3.8 Information About Website Visitors and Prospective Customers.

When you visit the Website, request a demo, or start a free trial, we collect the information you submit through our forms, such as name, email, phone number, and institution, together with the Usage Data described in Section 3.5.

4. How We Use Information

We use the information described in Section 3 to:

- provide, operate, maintain, and support the Service, including film analysis, tendency reports, scoring, rankings, and practice-plan generation;
- create and manage Customer and Authorized User accounts, and authenticate access to the Service;
- process payments, manage subscriptions, and send invoices and billing communications;
- respond to support requests, provide customer service, and communicate about the Service, including maintenance and security notices;
- monitor, secure, troubleshoot, and improve the performance, reliability, and functionality of the Service and Website, including through Usage Data and Aggregated and De-Identified Data;
- communicate with prospective customers about the Service, including responding to demo requests and trial sign-ups;
- comply with applicable law, respond to legal process, and enforce the Agreement, the DPA, and the AUP; and
- protect the rights, property, safety, and security of FalconEye, Customers, Authorized Users, and others.

FalconEye does not sell Personal Information, does not use Personal Information for targeted or cross-context behavioral advertising, and does not use Student Data or other Personal Information of a student-athlete to train, retrain, or improve any AI Technology except in Aggregated and De-Identified Data form.

5. Our Role as Service Provider/Processor; Customer as Controller

With respect to Personal Information contained in Customer Data, Customer is the data controller (or equivalent role under applicable law) and FalconEye acts solely as a service provider/processor, processing Customer Data only on Customer's documented instructions as set out in the Agreement and the DPA, and not for any independent purpose of its own. The customer is responsible for the lawful basis for its data and for any notices or consents required under applicable law. Individuals with questions or requests concerning Customer Data about them should, in the first instance, contact the relevant customer (school, club, or program); see Section 15.

With respect to information FalconEye collects directly and not as Customer's processor, such as Website visitor information, prospective-customer information, and the account or registration information of an individual coach or trainer who signs up directly with FalconEye rather than through an institutional Customer, FalconEye acts as the controller of that information for purposes of this Policy.

6. AI Features and Third-Party AI Technology

The Service includes AI Features that incorporate AI Technology to power film breakdown, scouting analysis, tendency tracking, scoring, ranking, and the Ask FalconEye assistant. These AI Features are provided in part through AI Technology made available by third-party providers, including foundation models offered by Google and Anthropic ("Third-Party AI Technology"). AI Customer Input is transmitted to these providers solely to generate AI Customer Output for Customer. FalconEye's agreements with its Third-Party AI Technology providers prohibit those providers from using AI Customer Input to train their own models for the benefit of other customers. FalconEye does not control, and is not responsible for, the underlying operation of Third-Party AI Technology.

7. How We Share Information

We share information only in the following circumstances:

- with subprocessors and service providers who help us operate the Service and Website (see Section 8), under contractual confidentiality, security, and data-protection obligations;
- within Customer's own organization, based on the access permissions Customer or its Admins configure for their Authorized Users;
- with Third-Party AI Technology providers, solely to generate AI Customer Output as described in Section 6;
- if required to comply with a subpoena, court order, or other valid legal process, or to protect the rights, safety, or property of FalconEye, our Customers, or others;
- in connection with a merger, acquisition, financing, reorganization, or sale of assets, subject to continued protection of Personal Information under materially equivalent privacy terms; and
- with Customer's consent, or as otherwise directed by Customer.

FalconEye does not sell Personal Information and does not share Personal Information for cross-context behavioral advertising.

8. Subprocessors

FalconEye engages third-party subprocessors to provide the Service, including for cloud hosting and infrastructure (currently Google Cloud Platform and Firebase, including Firestore, Cloud Storage, Authentication, and Realtime Database services), AI/ML processing (currently Google and Anthropic, as described in Section 6), payment processing (currently Authorize.Net), and transactional email delivery (currently Resend, which sends transactional email on FalconEye's behalf, with Google LLC's Gmail SMTP service used solely as the outbound routing and delivery layer for FalconEye's email domain). FalconEye requires its subprocessors to be bound by confidentiality and data-protection obligations. Certain payment-related intermediaries, such as the receiving bank for ACH settlement (currently M&T Bank Corporation), are included in the Subprocessor List for transparency only and do not process Personal Information. Subprocessor notice and objection procedures, where applicable, are governed by the DPA.

The current FalconEye Subprocessor List is available at <https://www.falconeyefaceoff.com/subprocessors> or upon request to chris@falconeyefaceoff.com.

9. Nest Rankings and Community Rankings

FalconEye may make available to holders of an active subscription a “Nest Rankings” list that displays a player’s name, school or program, and composite FalconEye Score. Consistent with Section 10, no individual under the age of 13 appears in the Nest Rankings. A Customer’s data is not included in the Nest Rankings unless the Customer affirmatively opts in by written request to chris@falconeyefaceoff.com.

10. Children’s Privacy; Eligibility; COPPA

The Service is intended for individuals who are 13 years of age or older, and FalconEye does not knowingly permit any individual under 13 to use the Service or knowingly collect personal information about a child under 13. The customer is responsible for not submitting information about any individual under 13, as set out in the Subscription Agreement and DPA. If FalconEye becomes aware that information relating to a child under 13 has been submitted to the Service, it will delete that information. Parents or guardians who believe their child’s information has been submitted may contact us at chris@falconeyefaceoff.com.

11. FERPA and Student Data

Some Customer Data may include student “education records” under the Family Educational Rights and Privacy Act (“FERPA”). FalconEye processes that data as a service provider on the Customer’s behalf and does not sell it or use it for targeted advertising. The parties’ specific FERPA responsibilities are governed by the Subscription Agreement and the DPA.

12. State Student Data Privacy Laws

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.

13. Data Security

FalconEye maintains administrative, technical, and physical safeguards designed to protect Personal Information against unauthorized access, use, disclosure, alteration, or destruction. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. FalconEye’s specific security commitments and its security-incident and breach-notification obligations to customers are governed by the Subscription Agreement and the DPA.

14. Data Retention and Deletion

FalconEye retains Customer Data for as long as Customer maintains an active subscription and thereafter deletes it from active systems within a commercially reasonable time, except for copies retained in routine backups or as required by law. Customer’s rights to access, export, or obtain return or deletion of Customer Data following termination are governed by the Subscription Agreement and the DPA, which control over this Policy. Account and billing information may be retained longer where necessary to comply with legal, tax, or accounting obligations. Aggregated and De-Identified Data, and Usage Data that does not identify

Customer or any individual, may be retained after termination and may be used and made publicly available by FalconEye in de-identified, non-identifying form.

15. Your Privacy Choices and Rights

Because most Personal Information relating to student-athletes, coaches, and staff is submitted to FalconEye by their school, club, or program (the data controller), individuals seeking to access, correct, or delete that information should direct their request to the relevant Customer in the first instance. FalconEye will reasonably assist Customer in responding to such requests, as described in the DPA. A Customer Admin may also request deletion of a Customer account directly by contacting chris@falconeyefaceoff.com; this action cannot be undone, so we recommend exporting your data first. An individual coach, trainer, or other user who registered directly with FalconEye, rather than through an institutional Customer, may contact us directly at chris@falconeyefaceoff.com to request access to, correction of, or deletion of their own account information.

16. Additional U.S. State Privacy Rights

A number of U.S. states have enacted comprehensive consumer privacy laws that give residents rights over their personal information, and the list of states with such laws continues to grow. These rights may include the right to access, delete, correct, or obtain a portable copy of personal information, and the right to opt out of the sale of personal information or its use for targeted advertising or certain profiling. FalconEye does not sell personal information and does not use personal information for targeted advertising, so opt-out rights of that nature are not generally applicable to FalconEye's processing. Where these rights apply, residents may submit a request to chris@falconeyefaceoff.com. We will take reasonable steps to verify identity before fulfilling a request, and a resident may designate an authorized agent to submit a request on their behalf.

17. California Privacy Rights (CCPA/CPRA)

If you are a California resident, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA/CPRA"), gives you the following rights with respect to your personal information: the right to know the categories and specific pieces of personal information we have collected about you and the categories of sources, purposes, and third parties involved; the right to delete personal information we have collected from you, subject to certain exceptions; the right to correct inaccurate personal information we maintain about you; the right to opt out of the "sale" or "sharing" of personal information (FalconEye does not sell or share personal information as those terms are defined under the CCPA/CPRA, and has not done so in the preceding twelve (12) months); the right to limit the use of sensitive personal information, which is not applicable because FalconEye does not use sensitive personal information for purposes that trigger this right in the ordinary course of providing the Service; and the right to non-discrimination for exercising any of the above rights.

Because most personal information relating to student-athletes is submitted to FalconEye by their school or program, California residents should generally direct requests concerning that data to the relevant school or program in the first instance. California residents may also submit requests directly to FalconEye at chris@falconeyefaceoff.com. We will take reasonable steps to verify your identity before fulfilling a request, and you may designate an authorized agent to submit a request on your behalf.

18. Do Not Track; Global Privacy Control

Some browsers offer a “Do Not Track” signal or support the Global Privacy Control (“GPC”). Because FalconEye does not sell personal information or use it for cross-context behavioral advertising, we do not currently respond differently to these signals. Where required by applicable law, we will honor a valid GPC signal as a request to opt out of any sale or sharing of personal information, to the extent such activity is applicable to our processing.

19. International Data Transfers

The Service and Website are hosted and operated in the United States. If Customer or its Authorized Users access the Service from outside the United States, information will be transferred to, stored, and processed in the United States, which may not have the same data-protection laws as the jurisdiction from which the information originated. The Service is designed for use by U.S.-based educational institutions, athletic programs, and trainers, and Customer is responsible for ensuring its use of the Service outside the United States complies with applicable local law.

20. Third-Party Links and Services

The Service and Website may contain links to third-party websites, applications, or services that FalconEye does not own or control, including any Third-Party AI Technology providers’ own websites. This Policy does not apply to those third-party sites and services, and FalconEye is not responsible for their privacy practices. We encourage you to review the privacy policy of any third-party site or service before providing information to it.

21. Changes to This Policy

We may update this Policy from time to time. If we make a material change, we will post the updated Policy and revise the “Last modified” date above, and provide any additional notice required by applicable law.

22. Contact Us

Questions, comments, or requests regarding this Policy or FalconEye’s data practices may be directed to:

FalconEye-Faceoff Intelligence System LLC

502 W 7th St STE 100

Erie, PA 16502

chris@falconeyefaceoff.com