

AccelEye Privacy Policy

Effective Date: August 21, 2026

This Privacy Policy explains how Accelx Inc., doing business as AccelEye ("AccelEye," "we," "us," or "our"), collects, uses, discloses, and protects personal information across all of our products and services, including: our marketing website; our AI-powered weapon and violence detection service, which analyzes security camera video feeds ("Detection Service"); the AccelEye Safety Agent browser extension for school-managed Chromebooks and Google Workspace accounts ("Safety Agent"); the SaveAlert mobile app; and any purchase made through our online ordering system. This Privacy Policy applies to all users of these products and services, including school districts, school personnel, students and their parents/guardians, and website visitors.

1. Information We Collect

Website visitors and trial users

If you register to trial our website, apps, or components, we collect the email address and username you select. We recommend choosing a username that is not your real name. You may also select a password, and may optionally share your general geographic location, occupation, and interests; none of this optional information is required to register.

Customers purchasing a service

If you purchase a service through our online ordering system, we collect your name, shipping address, billing address, payment card information, email address, and phone number, in order to process your purchase and contact you about it. We do not store payment card information on our own servers; our payment processor stores this information to handle recurring payments, refunds, and chargebacks. We do not use this information for any purpose other than processing your purchase and will not share it with any other third party, except as described in this Policy or as required by law. We will only use your email address for marketing if you affirmatively opt in during checkout, and you may withdraw that permission at any time (see "Contact Us" below).

School personnel

When a school administrator registers a school with AccelEye or corresponds with us, we collect a contact name, school name and district, school email address, school physical address, phone number, job title, message content, and information about the school's information systems. Once a school begins using our Services, we keep records of related account and support activity.

Student data (Safety Agent)

Where a school deploys the Safety Agent browser extension, we may access student name, email address, device information/identifiers, content from school-approved educational platforms (such as Google Classroom, Gmail, and Google Docs), and related usage data, solely to provide student-safety insight and reporting services the school has authorized. Students never register for or interact directly with AccelEye; every account and every authorization comes from the school. Except where a threat indicator is detected, AccelEye does not retain the underlying content it scans.

Video, image, and biometric-adjacent data (Detection Service)

AccelEye's core Detection Service analyzes video feeds from security cameras a school or venue already operates, to identify potential weapons or violent activity and route verified alerts to authorized personnel and, where configured, emergency services.

Because this is passive analysis of camera feeds, AccelEye may process images of any person who appears on camera — students, staff, and visitors alike — not only individuals who hold an account or username.

Video and images of children have been regulated "personal information" under COPPA since 2013. AccelEye's AI outputs relating to this footage (for example, indications used for weapon or facial-recognition-adjacent detection) may also be "biometric information" under certain state laws; see "Biometric Data" below.

AccelEye's use of school security-camera footage relies on the school's authority to authorize the service for a school-safety purpose, consistent with FTC guidance recognizing schools as an appropriate consenting party for education-technology and school-safety services used in the educational context and not for unrelated commercial purposes.

We do not use video, image, or biometric-adjacent data for advertising, marketing, or unrelated profiling of any individual.

We also do not use a school's video or image data to train or develop AccelEye's AI models; see "Use of children's data to train AI models" below for how our models are trained.

Device, usage, and cookie data

We may collect device and usage information such as IP address, device identifiers, browser and operating-system type, access times, and which parts of our website or app are used, from any visitor, school-managed device, or app user. We may use cookies and similar technologies, including cookies placed by third parties for website analytics, to understand and improve our website; we do not use cookies to target advertisements to specific users, and any third party placing analytics cookies is contractually prohibited from sharing personally identifiable information it collects with anyone other than AccelEye, except as required by law.

2. Children's Privacy (COPPA)

AccelEye complies with the Children's Online Privacy Protection Act (COPPA) and its 2025 amendments. Students do not, and cannot, register for or sign up to any AccelEye product themselves. Every student account or authorization is provisioned by a verified educator, school, or educational organization, which agrees to obtain and maintain all consents COPPA requires — from the student's parent or legal guardian where necessary — before a student is given access to, or is processed by, our Services.

- We do not collect online or offline contact information from a child without consent from a parent, qualified educator, or educational institution.
- We do not use or disclose a child's information, including video or image data, for behavioral advertising, and we do not build personal profiles of students except for authorized educational or school-safety purposes.
- Consistent with the 2025 amendments, we treat biometric identifiers (including facial recognition data) as personal information subject to these same commitments.
- We retain children's personal information only for the minimum time necessary for the purpose it was collected, and implement secure disposal procedures once that period ends.

AccelEye's detection models are trained exclusively on publicly available data and fully anonymized data. AccelEye does not use any child's personal information, or any other individually identifiable information collected through our Services (including video or image data captured by a school's security cameras), to train or develop its AI models. Because no personal information is used for this purpose, the 2025 amendments' AI-training consent requirement is not triggered by AccelEye's model-training practices.

This is distinct from AccelEye's use of a school's live camera feed to operate the Detection Service for that school, which is addressed in "Video, image, and biometric-adjacent data" above and relies on the school's authorization, not on AccelEye's model-training practices. If AccelEye's practices change so that identifiable data is ever used to train a model, we will update this Policy and obtain separate opt-in parental consent before doing so.

3. FERPA

For services provided to schools, AccelEye operates under FERPA's "school official" exception, with a legitimate educational interest in the student-safety insights and educational-environment protections our Services provide. School districts maintain control of student data; we act under their direction, and we have no direct relationship with students or parents outside of that direction.

4. How We Share Information

We share personal information only as described below, and we do not sell personal information or use it for any commercial purpose beyond providing and improving our Services.

- Service providers (sub-processors) that host, process, or support our Services on our behalf, such as cloud hosting and analytics providers, bound by confidentiality and data-protection obligations in our contracts with them.
- Authorized school personnel, at the direction of the school, or to facilitate a service the school has requested.
- Emergency services and law enforcement, when a verified threat alert requires it, or otherwise as required by law.
- Payment processors, solely to process a purchase you make through our online ordering system.
- With your consent, or the consent of (or at the direction of) a parent, guardian, or eligible student.

Disclosures to service providers under the categories above are made under contracts that satisfy the CCPA/CPRA "business purpose" exception; AccelEye does not consider, and does not treat, these disclosures as a "sale" or "share" of personal information as those terms are defined under California law.

5. Biometric Data

Because our Detection Service performs AI-based visual analysis of security-camera footage, certain outputs may be considered biometric identifiers or biometric information under state law, including the Illinois Biometric Information Privacy Act (BIPA), the Texas Capture or Use of Biometric Identifier Act (CUBI), and Washington's biometric privacy law (RCW 19.375).

- We collect and process biometric identifiers only as necessary to provide contracted threat-detection and safety services, pursuant to a school district's or customer's authorization.
- We do not sell, lease, trade, or otherwise profit from biometric identifiers or biometric information.
- We retain biometric data only as long as necessary for the purpose it was captured, consistent with the retention schedule below, absent a legal hold, and maintain a written policy governing its permanent destruction, available on request.

6. Cookies, Do Not Track, and Global Privacy Control

See "Device, usage, and cookie data" above for the cookies we and our analytics partners use. AccelEye honors the Global Privacy Control (GPC) signal, and any other universal opt-out preference signal recognized under applicable state law, as a valid request to opt out of the sale or sharing of personal information from the browser or device sending the signal. Because we do not sell or share personal information as those terms are defined by the CCPA/CPRA, honoring a GPC signal currently has no practical effect on our processing, but we will continue to recognize it as required by law as our practices evolve.

7. Data Retention

- Account data: for the duration of the active account, plus 30 days after closure, unless a longer legal retention period applies.

- Security-event video/image data: retained for 90 days from capture, or longer where required for an active investigation or a law-enforcement request.
- Digital threat-analysis data (Safety Agent content flags): 90 days, or longer where required for an active investigation.
- School/account records: retained for a commercially reasonable time after account closure for backup, archival, or audit purposes; all associated student data is deleted per AccelEye's Data Deletion policy.
- Audit logs: a minimum of 2 years for security and compliance purposes.

After the applicable retention period, we securely delete or anonymize personal data unless a longer period is required by law or an active legal hold applies.

8. Security

We implement administrative, technical, and physical safeguards designed to protect the personal information we collect, including encryption in transit and at rest, multi-factor authentication, role-based access control, regular security assessments, an incident response plan, and privacy/security-by-design review of new products and features. While we take the security of your information seriously, no method of transmission or storage is completely secure, and we cannot guarantee absolute security.

9. Incident & Breach Notification

If we discover a breach of security involving personal information, we will notify the affected school district, customer, or individual without unreasonable delay, and in all cases within the timeframe required by applicable law, including the specific notification-content and timing requirements of the state law that applies to each affected individual.

10. Legal Basis for Processing

- Consent, to respond to an inquiry you submit or to provide a service you have requested.
- Legitimate interest, for the proper administration, security, and monitoring of our products and website.
- Performance of a contract with the school, district, or customer that has subscribed to our Services.
- Compliance with a legal obligation, including responding to lawful requests from public authorities.

11. Your California Privacy Rights (CCPA/CPRA)

Your rights

- Right to Know: the categories of personal information we collect or disclose, our sources, our business purpose, and the categories of third parties we share it with.
- Right to Access: a copy of the specific personal information we hold about you, subject to limited statutory exceptions.
- Right to Delete: deletion of personal information we hold about you, subject to legal retention requirements.
- Right to Correct: correction of inaccurate personal information.
- Right to Limit Use and Disclosure of Sensitive Personal Information.
- Right to Opt-Out of the sale or sharing of personal information (see Section 6 — we do not currently sell or share personal information).
- Right to Non-Retaliation for exercising any of the above rights.

Sensitive personal information

Depending on the AccelEye product a school uses, sensitive personal information we may process includes precise geolocation (for school-managed devices) and biometric-adjacent information generated by our Detection Service. We use sensitive personal information only to provide the contracted Service, and do not use it to infer characteristics about an individual for any other purpose.

How to exercise your rights

Categories collected and disclosed (preceding 12 months)

Category of Personal Information	Categories of Third Parties Disclosed To
Identifiers (name, email, unique user ID)	Service providers, authorized school personnel
Educational records	Authorized school personnel, service providers (under confidentiality obligations)
Video, image, and biometric-adjacent information	Authorized school personnel, emergency services (where a threat is verified), service providers
Device information and identifiers	Service providers, authorized school personnel
Internet or electronic network activity	Service providers, authorized school personnel
Geolocation data (school devices only)	Authorized school personnel, service providers
Payment information (purchasers only)	Payment processor

We do not "sell" or "share" California residents' personal information as those terms are defined under the CCPA/CPRA, and we do not share personal information with third parties for their own direct marketing purposes (California "Shine the Light").

12. Your Privacy Rights in Other U.S. States

AccelEye provides services to school districts, and processes personal information of residents, across the United States. This section summarizes rights and protections beyond California.

Comprehensive state consumer privacy laws

As of 2026, roughly twenty states have enacted comprehensive consumer privacy laws generally modeled on the CCPA/CPRA and Virginia's Consumer Data Protection Act, including, among others, Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Florida, Montana, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Kentucky, Indiana, Rhode Island, Tennessee, Minnesota, and Maryland, with more states enacting laws or amendments each year. To the extent these laws apply to you, AccelEye extends the same core rights described in Section 11 above — to know, access, correct, delete, and opt out — and does not sell personal information.

State student data privacy statutes

Virtually every U.S. state has enacted some form of student data privacy law, and a large majority — including, among others, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Iowa, Kansas, Maine, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oregon, Texas, and Utah — follow the general model established by California's SOPIPA, restricting targeted advertising to students, sale of student data, and non-educational student profiling. Our practices described throughout this Policy (no sale of student data, no targeted advertising, no non-educational profiling, school/district control of data) are designed to satisfy these statutes generally. New York's Education Law § 2-d and New Mexico's student data governance standards receive their own detailed treatment in AccelEye's Compliance Statement.

State data breach notification laws

All fifty states, the District of Columbia, and several U.S. territories have breach-notification statutes. Our commitments in Section 9 are designed to meet the notification content and timing requirements of the law applicable to each affected individual.

State audio consent-to-record laws

Where any AccelEye hardware or software captures audio in addition to video, we comply with applicable state consent-to-record laws, including the roughly one-third of states that require the consent of all parties to a recorded conversation. Schools and districts should confirm with their AccelEye representative whether a given deployment captures audio.

13. International Users: EU, UK, and Switzerland

For personal data received from the European Union, European Economic Area, United Kingdom, or Switzerland, AccelEye is in the process of self-certifying to the U.S. Department of Commerce under the EU-U.S. Data Privacy Framework, the UK Extension, and the Swiss-U.S. Data Privacy Framework. AccelEye's Data Processing Agreement, including Standard Contractual Clauses and the UK International Data Transfer Addendum, currently serves as the operative transfer mechanism for any such data. This statement will be updated with our certification date and DPF Participant List entry as soon as certification is complete. For the complete set of GDPR/UK GDPR commitments and rights available to international users, see AccelEye's Data Privacy Framework Privacy Policy.

14. How to Access or Correct Your Data

Adult end users and school personnel should contact their educational institution about accessing or correcting data collected and used by AccelEye on the institution's behalf, or may sign into an administrator account directly. Student end users and their parents should contact their school about access to personal information collected by that institution. School districts and other AccelEye customers may also contact us directly at privacy@acceleye.com.

15. Governing Law & Dispute Resolution

This Privacy Policy is governed by the laws of the State of California, without regard to its conflict-of-laws principles, except where a different jurisdiction's law is required to apply to your rights (for example, under the GDPR or another state's privacy statute). Any dispute arising from this Policy will be handled as described in AccelEye's Terms & Conditions. This section does not limit any right you have under a mandatory consumer-protection or data-protection law that cannot be waived by agreement.

16. Other Websites

Our site contains links to other websites. We are not responsible for the privacy practices or content of those other sites.

17. Changes to This Policy

We may update this Privacy Policy periodically to reflect changes in our data practices or in applicable law. We will post the updated Policy on our website with a new "Effective Date," and, for material changes affecting school districts, will provide notice consistent with our contractual obligations.

18. Contact Us

Publisher: Accelx Inc. (d/b/a AccelEye)

Business Address: 447 Downing Ave, San Jose, CA 95128, USA

Privacy & Data Rights Requests: privacy@acceleeye.com

General Support: support@acceleeye.com | +1 (844) 755-4837

Response Time: 24-48 hours for general privacy inquiries; see Section 11 for CCPA/CPRA statutory timelines.

Effective Date: August 21, 2026

This Privacy Policy is maintained by Accelx Inc. (AccelEye)'s Legal and Privacy Team and is reviewed at least quarterly for compliance with evolving regulations.