AccelEye Data Privacy, Security & AI Compliance Statement

We take data privacy and security seriously.

Important Notice: System Limitations

AccelEye's AI-powered detection technology is designed to help identify potential weapon and violence threats from security camera feeds and to accelerate human review, verification, and emergency response. It is a risk-mitigation and response-time tool.

No detection technology, including AccelEye's, can identify every threat in every circumstance, and no technology can guarantee the prevention of harm, injury, or loss of life. AccelEye's system is designed to operate alongside, and not as a replacement for, trained personnel, school safety protocols, law enforcement, and existing physical security measures.

Detection results are subject to human verification before dispatch of an alert, and performance can be affected by factors including camera placement, lighting, obstruction, network connectivity, and the inherent limitations of AI-based image analysis.

AccelEye's Artificial Intelligence (AI) Ethics & Principles

AccelEye recognizes the transformative potential of artificial intelligence in technology and business. We are committed to the responsible and ethical use of AI, ensuring that our solutions maximize benefits while serving our customers' best interests. Our AI ethics framework aligns with our core values and professional standards, and with recognized frameworks such as the NIST AI Risk Management Framework, building trust with our clients, communities, and regulatory authorities.

We uphold our commitment to act in the public interest, respect public trust, and demonstrate professional excellence in all AI implementations, including regular testing intended to reduce false positives and false negatives in threat detection over time.

For more information, please see our *Responsible Use of AI Policy*.

How AccelEye Collects Data: Security Camera Video & Image Analysis

AccelEye's core service analyzes video feeds from security cameras already deployed by a school or district to detect potential weapons or violent activity, and to route verified alerts to authorized school personnel and, where configured, emergency services. Unlike a typical software account, this means AccelEye's AI may process images of any person — student, staff, or visitor — who appears on camera, not only individuals who hold a login or "account."

Legal basis for processing images of students

- AccelEye's camera-based services are deployed by a school or district in its capacity as the data holder and, for COPPA purposes, may rely on the school's authority to consent on behalf of parents for use of an education technology service within the school context, consistent with FTC guidance recognizing schools as an appropriate consenting party where the service is used solely for a school-authorized educational or school-safety purpose and not for commercial purposes unrelated to that use.
- Video and images of children are, and have been since 2013, regulated "personal information" under COPPA. AccelEye does not use video or image data collected through school security cameras for any commercial, advertising, or profiling purpose.
- Video/image data captured for threat detection is retained only as long as necessary for safety, investigative, and legal purposes as described in "Data Retention" below, and is not used to build behavioral or marketing profiles of any individual.

Audio

Where any AccelEye hardware or software captures audio in addition to video, AccelEye complies 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.

Children's Online Privacy Protection Act (COPPA)

Rule Effective Date: June 23, 2025 (2025 Amendments). **Compliance Deadline:** April 22, 2026 for most amended provisions, per the FTC's Federal Register notice published April 22, 2025. AccelEye has been in full compliance with the amended Rule since that deadline.

The Children's Online Privacy Protection Act (COPPA) applies to the online collection of personal information from children under 13 by persons or entities under U.S. jurisdiction, and requires verifiable parental consent (or, in the school context, consent obtained through the school as described above) for the collection, use, or disclosure of personal information from children.

AccelEye's COPPA Compliance

AccelEye complies with COPPA and its 2025 amendments. Where AccelEye products involve individual student accounts, accounts are provided exclusively through verified educators, schools, or educational organizations, and educators agree to obtain appropriate parental permission before issuing accounts to students. Where AccelEye products involve passive camera-based detection rather than individual accounts, AccelEye relies on the school's authority to authorize the service for a school-safety purpose as described above.

Our COPPA Commitments

Data Collection

- We will NOT collect online or offline contact information without consent from a parent, qualified educator, or educational institution.
- We will NOT collect personally identifiable information without proper authorization.
- Consistent with the 2025 amendments, we treat biometric identifiers (including fingerprints, voiceprints, and facial recognition data) as personal information subject to these commitments.

Data Use and Disclosure

- We will NOT distribute personally identifiable information to third parties without prior parental (or school, where legally authorized) consent.
- We will NOT use or disclose student information, including video or image data, for behavioral targeting of advertisements.
- We will NOT build personal profiles of students except for authorized educational or school-safety purposes.
- We require separate opt-in parental consent before sharing children's data for targeted advertising (a use case AccelEye does not currently engage in).

Data Protection (2025 Requirements)

- We maintain a comprehensive written Information Security Program with administrative, technical, and physical safeguards protecting children's data.
- We retain children's personal information, including video/image data, only for the minimum time necessary to fulfill the purpose for which it was collected.
- We implement secure data disposal procedures when retention is no longer required.

Incentives

- We will NOT entice children to divulge more information than necessary by offering special games, prizes, or activities.

Contact AccelEye for a Complete COPPA Notice

Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law protecting the privacy of student education records. It applies to schools receiving funds under applicable U.S. Department of Education programs.

AccelEye's FERPA Compliance

Although FERPA applies directly to schools rather than to vendors, AccelEye may be designated as a “School Official” with a legitimate educational interest under FERPA when providing services to a district. In that capacity, we comply fully with FERPA's requirements and protect the privacy of student information entrusted to us by school districts.

Key Commitments

- School districts maintain control of all student data; we operate under their direction.
- We support parents' and eligible students' rights to access, inspect, review, and seek correction of education records, exercised through the school district.
- We respond to verified written requests from school districts within the timeframes required by FERPA and by our agreements with each district.
- We implement appropriate security measures to protect education records, including video and image data that constitutes an education record.

> **Note**
>
> AccelEye does not have direct contact with students or parents. All interactions regarding student data occur through authorized school officials.

New York Education Law § 2-d

New York Education Law § 2-d, and its implementing regulations at 8 NYCRR Part 121 adopted by the Board of Regents, protect the privacy and security of personally identifiable information (PII) of students, classroom teachers, and principals.

AccelEye's NY Education Law § 2-d Compliance

AccelEye complies with NY Education Law § 2-d, 8 NYCRR Part 121, and the Parents' Bill of Rights for Data Privacy and Security.

Required Protections

- Student PII cannot be sold or released for commercial purposes.
- Parents have the right to inspect and review their child's complete education records.
- We implement industry-standard safeguards, including encryption, firewalls, and password protection, when storing or transferring student PII.
- We provide breach notification in accordance with applicable laws and our Data Protection Agreements with districts.
- We address parental complaints about possible data breaches, in coordination with the relevant school district.
- Our staff handling PII receive training on federal and state law, policy, and industry best practices.
- Our contracts with educational agencies (including a signed Parents' Bill of Rights supplement) address the statutory and regulatory data privacy and security requirements of § 2-d and Part 121.

Nationwide Coverage: Other U.S. State Laws

AccelEye provides services to school districts across the United States. Beyond New York and New Mexico (each addressed in its own section), the sections below describe how AccelEye approaches the other categories of state law most relevant to its products, on a nationwide basis. Because state privacy legislation changes frequently, AccelEye's Legal and Privacy Team maintains a current, state-by-state compliance matrix, available to customers on request at privacy@acceleye.com.

State student data privacy statutes (all 50 states)

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 Student Online Personal Information Protection Act (SOPIPA), restricting targeted advertising to students, the sale of student data, and the creation of non-educational student profiles. AccelEye's practices described throughout this statement (no sale of student data, no targeted advertising, no non-educational profiling, school/district control of data) are designed to satisfy these statutes generally. Where a specific state or district requires its own addendum or certification, AccelEye will execute it; contact privacy@acceleye.com.

Comprehensive state consumer privacy laws

As of 2026, approximately twenty U.S. states have enacted comprehensive consumer privacy laws generally modeled on the CCPA/CPRA and Virginia's Consumer Data Protection Act framework (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 additional states enacting new laws or amendments each year. For business contacts, employees, and any consumer personal data outside the school-services context, AccelEye extends the same core rights described in the CCPA/CPRA section above — the rights to know, access, correct, delete, and opt out — to residents of these states to the extent each state's law applies, and does not sell personal data.

State data breach notification laws

All fifty states, the District of Columbia, and several U.S. territories have breach notification statutes. AccelEye's Incident & Breach Notification commitments (below) are designed to meet the notification content and timing requirements of the state law applicable to each affected individual, in coordination with the school district or customer responsible for the underlying notification obligation.

State biometric privacy and wiretap/consent-to-record laws

See “Biometric Data Practices” above for state biometric statutes, and “How AccelEye Collects Data” above for state audio consent-to-record laws. Both are evaluated on a state-by-state basis for every AccelEye deployment.

Biometric Data Practices

Because AccelEye's technology performs AI-based visual analysis of security camera footage, we recognize that certain outputs of that analysis may be considered biometric identifiers or biometric information under state law, including statutes such as 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), as well as biometric provisions found in comprehensive state privacy laws.

- We collect and process biometric identifiers only as necessary to provide contracted threat-detection and safety services, and only 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 safety, investigative, or legal purpose for which it was captured, and in no case longer than our published retention schedule below, absent a legal hold.

- We maintain a written policy governing the retention and permanent destruction of biometric data, available to customers upon request.

New Mexico Student Data Privacy Compliance

AccelEye is committed to protecting the privacy and security of student data in compliance with all applicable New Mexico requirements. While New Mexico does not currently have a standalone student data privacy statute, AccelEye adheres to FERPA, COPPA, and the data governance standards established under NMSA § 22-1-11 by the New Mexico Public Education Department (NMPED). AccelEye actively participates in the Student Data Privacy Consortium (SDPC) and works with New Mexico school districts to execute National Data Privacy Agreements (NDPAs) establishing clear expectations for data collection, use, security, and deletion. Student data processed by AccelEye is used solely for authorized school-safety purposes, is never sold or used for commercial advertising, and is protected by industry-standard encryption, access controls, and breach notification procedures. School districts maintain full ownership and control of all student data, and AccelEye retains information only for the minimum time necessary to fulfill its school-safety mission.

Student Data Privacy Consortium (SDPC) and National Data Privacy Agreement (NDPA)

The SDPC's National Data Privacy Agreement (NDPA) streamlines contracting between schools/districts and marketplace providers while establishing common data privacy expectations.

- AccelEye works with school districts in all participating states to execute Data Processing/Privacy Agreements.

privacy@acceleye.com

- The SDPC represents a collaboration among schools, districts, regional agencies, territories, state agencies, policymakers, trade organizations, and marketplace providers addressing real-world, implementable solutions to data privacy concerns.

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

Effective Date: January 1, 2023 (CPRA amendments to CCPA). Most recent amendments: 2025.

CPRA amends and significantly expands the CCPA, protecting personal data of California employees (B2E), business-to-business (B2B) contacts, and California residents.

Who CPRA Protects

- A California resident employee.
- A service provider, vendor, contractor, consultant, applicant, freelancer, or remote worker reasonably identifiable as a California resident.

California Employee & B2B Data Rights

- **Right to Know:** what personal data is collected and managed, including access to specific pieces of personal information.
- **Right to Access:** submit a Data Subject Access Request (DSAR), subject to limited statutory exceptions.
- **Right to Limit Use and Disclosure:** request that we limit or stop using and disclosing sensitive personal information.
- **Right to Correct:** request correction of inaccurate information.
- **Right to Opt-Out:** opt out of the sale or sharing of personal information.
- **Right to Non-Retaliation:** individuals cannot be retaliated against for exercising any data right.

AccelEye's CCPA & CPRA Compliance Program

- Data Mapping: we maintain a comprehensive mapping, inventory, and classification of personal data.
- Data Minimization: we process only data that is adequate, relevant, and limited to what is necessary for specified purposes.
- Data Retention: we implement data retention schedules across all products and processes; see “Data Retention” below.
- Privacy Impact Assessments: we conduct risk assessments of products and processes to support privacy and security by design.
- AI-Specific Protections (AB 1008): we apply CCPA's privacy protections to our generative-AI-adjacent processing consistently with other data storage, processing, and use.
- Neural Data Protection (SB 1223): we treat “neural data” as sensitive personal information where applicable.
- Transaction Compliance (AB 1824): we maintain consumer opt-out preferences through mergers, acquisitions, bankruptcy, or other corporate transactions.

General Data Protection Regulation (GDPR) and UK GDPR

Effective Date: May 25, 2018 (GDPR); January 1, 2021 (UK GDPR).

The GDPR and UK GDPR establish comprehensive rules for collecting, using, storing, and transferring personal data of individuals in the European Union and United Kingdom. For products delivered to schools and districts, AccelEye acts as a Data Processor, processing personal data only on documented instructions from the Data Controller (the school or district).

AccelEye's GDPR Compliance Program

- Processing only on documented controller instructions, with staff confidentiality obligations, support for Data Protection Impact Assessments, and assistance with data subject rights requests (Article 28).
- A Data Processing Agreement including EU Standard Contractual Clauses and the UK International Data Transfer Addendum, covering processing scope, security measures, breach notification, audit rights, and sub-processor management. To execute a DPA, contact privacy@acceleye.com.
- Data minimization and purpose limitation — no use for advertising or unrelated profiling, and no sale of personal data.
- A current, maintained Records of Processing Activities (ROPA) under Article 30.
- Technical and organizational security measures under Article 32, including encryption in transit and at rest, MFA, role-based access control, and a vulnerability management program.
- Privacy by Design and Default under Article 25, including default-off or scoped data-collection features.
- Breach notification to controllers without undue delay, supporting the controller's own 72-hour supervisory-authority notification obligation under Articles 33–34.

Data Privacy Framework (DPF) Certification

Certification status: in process

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 to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework.

AccelEye's Data Processing Agreement, including Standard Contractual Clauses and the UK IDTA, currently serves as the operative transfer mechanism for any personal data received from the EU, UK, or Switzerland.

This statement will be updated with AccelEye's certification date and a link to our listing on the DPF Participant List as soon as certification is complete.

Office of Foreign Assets Control (OFAC) Compliance

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security objectives.

AccelEye's OFAC Compliance Program

AccelEye, Inc., its subsidiaries, and affiliates are committed to full compliance with applicable international sanctions, including those imposed by the United States, the European Union, the United Kingdom, and the United Nations.

- Screening: we screen international orders and customer engagements against comprehensive lists of sanctioned and prohibited persons and destinations before acceptance.
- Prohibited Transactions: we reject any order or engagement, directly or indirectly, involving a sanctioned person, sanctioned entity, or sanctioned destination.
- Training: AccelEye personnel receive annual OFAC and export-control awareness training.
- Export Controls: we maintain a documented export-controls compliance program integral to our business operations and code of conduct.

SOC 2 Compliance

Certification status: audit in process

AccelEye designs and operates its products and internal controls to meet the AICPA's SOC 2 Trust Services Criteria (security, and, where applicable, availability and confidentiality).

AccelEye's SOC 2 audit is currently in process and has not yet resulted in an issued report. AccelEye does not yet hold a completed SOC 2 certification and does not represent otherwise.

This statement will be updated with the audit type (Type I or Type II), the report period, and instructions for requesting a copy of the report under NDA, as soon as the audit is complete.

DHS SAFETY Act Designation

The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 allows the U.S. Department of Homeland Security to designate or certify qualifying anti-terrorism technologies, providing important legal protections — including liability limitations — to sellers and users of those technologies.

Designation status: application in process

AccelEye has applied to the DHS Office of SAFETY Act Implementation for SAFETY Act protection for its weapon and violence detection technology. This application is currently in process and has not yet resulted in an approved Designation or Certification.

AccelEye does not yet hold SAFETY Act Designation or Certification and does not represent otherwise.

This statement will be updated with the approval date, the specific protection level granted, and the applicable coverage period as soon as DHS issues a determination.

Our Data Security Program

Administrative Safeguards

- A designated privacy and security compliance team and Data Protection Officer.
- Documented privacy and security policies and procedures, with recurring staff training.

- Background checks for personnel with access to personal data, where permitted by law.
- Documented incident response and breach notification procedures.

Technical Safeguards

- Encryption in transit (TLS 1.2+) and at rest (AES-256).
- Multi-factor authentication (MFA) and role-based access control (RBAC) on the principle of least privilege.
- Regular security assessments, vulnerability management, and penetration testing.
- Intrusion detection/prevention, comprehensive logging and monitoring, and a secure software development lifecycle.

Physical Safeguards

- Data centers with 24/7 security, surveillance, and access controls.
- Controlled access to facilities and equipment handling personal data.

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 by law enforcement request.
- Digital threat-analysis data: 90 days, or longer where required for an active investigation.
- Audit logs: a minimum of 2 years for security and compliance purposes.

After the applicable retention period, AccelEye securely deletes or anonymizes personal data unless a longer retention period is required by law or an active legal hold.

Incident & Breach Notification

If AccelEye discovers a breach of security involving personal data, we will notify the affected school district or customer without unreasonable delay, and in all cases within the shortest timeframe required by applicable state or federal law, so that the district can meet its own notification obligations to parents, students, and staff. We will provide the nature and scope of the incident, the categories of data involved, and the remediation steps taken, and will cooperate with the district's and any regulator's investigation.

Your Rights & How to Contact Us

Parents and eligible students should direct requests to access, correct, or delete education records to their school or district, which will coordinate with AccelEye as needed. School districts, and individuals exercising rights under CCPA/CPRA, GDPR, or other applicable law, may contact AccelEye directly using the information below.

Privacy and Compliance Inquiries: privacy@acceleye.com
Data Processing Agreements: privacy@acceleye.com
Data Subject Rights Requests: privacy@acceleye.com
General Support: support@acceleye.com | +1 (844) 755-4837
Data Protection Officer: Alimul Hoque — privacy@acceleye.com

Document Version: 3.0
Last Updated: August 21, 2026
Next Review Date: November 21, 2026
This document is maintained by Accelx Inc. (AccelEye)'s Legal and Privacy Team and is reviewed at least quarterly for compliance with evolving regulations.