



Let's Build Canadian Football, Together.

BROUGHT TO YOU BY ASCENSION MEDIA GROUP INC.

Information for School Boards and Athletic Departments

This document is prepared for school administrators, athletic directors, IT departments, and procurement officers reviewing ALL24 for use by school-based football programs. It summarizes the platform, the data model, the privacy and security posture, and answers questions commonly raised during institutional review.

ALL24 recognizes that school programs operate in a more administratively scrutinized environment than independent club programs, and we have designed the platform — and these accompanying materials — with that reality in mind.

At a glance

Operator: Ascension Media Group Inc., an Ontario corporation. Registered address: 114 Gemini Drive, Hamilton, ON L9C 6C4.

Product: ALL24 — a closed, team-scoped coaching platform for film review, playbook design, and team communications. Built specifically for Canadian football.

Users: Coaches, team staff, and players aged 13 and older. Each team operates in a private environment; no cross-team visibility, no public profiles.

Pricing model: Annual subscription per team, billed via invoice (no automatic charges). Pricing aligned with the Canadian school year.

Compliance footing: PIPEDA-compliant. Designed to align with MFIPPA (Ontario), FIPPA, FOIP (Alberta), FOIPPA (BC), and Quebec Law 25 where school boards are involved. Minimal data collection — name and email address only from each user, plus team-related metadata (position, jersey number).

Where data lives: User account data (names, emails, attestations, team memberships, chat messages, watch history) and the application server are both hosted on **OVH** infrastructure in **Beauharnois, Quebec, Canada**. Some media storage and transient video processing occurs in mixed regions or the United States — disclosed in detail below and in the Privacy Policy.

Legal documents: [Terms of Service](#), [Privacy Policy](#), and [Team Agreement](#) are publicly available at all24.ca. The full [Security Summary](#) is published; the **Data Processing Agreement (DPA)**, **Privacy Impact Assessment (PIA)**, **Privacy Breach Notification Process**, and **Incident Response Process** are available on request through a one-time secure link — email privacy@all24.ca or legal@all24.ca with your role and institution.

Data collected

From every user

- Full name
- Email address
- Profile avatar (optional, user-uploaded)
- Roster information: team, position, jersey number, role designations such as captain status
- Attestation records (age 13+, parental permission for users under 18, acceptance of legal documents)
- IP address at login (for security and authentication)
- Usage data: features accessed, film clips viewed, viewing timestamps

Not collected

- Date of birth or specific age
- Home address
- Phone number
- Academic records, grades, or school identifiers
- Health, medical, or accessibility information
- Government-issued identifiers
- Any data from users under 13 (the platform is age-gated at 13+)

Billing data

Subscription billing information is collected and processed directly by **Stripe** under its own privacy practices. AMGI does not receive or store payment card information. Billing is invoice-based and only the team's designated billing contact provides payment details — players and parents do not.

User lifecycle and access control

ALL24's user lifecycle is designed around three principles: every user actively consents to the platform, every team controls who joins, and users retain the ability to leave and delete their data at any time.

Registration

- Users cannot register without a team-issued join code or invite link. Public registration is not available.
- At registration, every user attests to (a) being 13 or older, (b) having parental or guardian permission if under 18, and (c) acceptance of the Terms of Service and Privacy Policy. Each attestation is recorded with timestamp, IP address, and the version of the legal document in effect at the time.
- Registration places the user in a "pending" state. The team's coach or administrator must review and approve before the user gains access to team content.

Approval audit trail

- Every approval is logged: which coach approved the user, when, and via what method.
- Per-player compliance records are available on request to privacy@all24.ca and include the user's registration date, attestation history, and the verbatim text of every legal document the user accepted at the time of acceptance.
- Schools can use these compliance records as part of their own consent and onboarding documentation.

Departure and removal

- Users can leave any team at any time from their account settings. Coaches can remove users from their team at any time.
- On user-initiated departure, team-scoped data (chat messages, watch history) enters a 14-day grace period during which the user can rejoin and have it restored, then is permanently stripped.
- On coach-initiated removal, the user's access is revoked immediately. Team-scoped data enters a 48-hour reinstate window for correction of mistakes, then is permanently stripped.
- Users can delete their account entirely with a 30-day grace period for restoration.
- Inactive accounts are auto-deleted after defined retention windows: 90 days for never-joined accounts, 12 months from last activity for previously-attached accounts.

Right to data access

Every user can download a complete archive of their account from **Settings → Privacy → Download my data**. The archive is a ZIP file containing JSON-per-section (account, attestations with verbatim agreement text, messages authored, login history, watch history, playlists, attachments, reports filed) plus a human-readable summary that can be saved as a PDF using the browser. This implements PIPEDA Principle 9 (Individual Access) and the equivalent rights under provincial privacy laws.

Security

- Encryption in transit: TLS 1.2 or higher on every connection
- Encryption at rest: **two layers**.
 - Layer 1: database-wide AES-256 tablespace encryption via MariaDB's [file_key_management](#) plugin. Every database file on disk — including data files, redo log, binary log, Aria tables, temporary files — is encrypted. A copy of the raw database directory yields no readable user data without the encryption key.
 - Layer 2: application-level AES-256-GCM column encryption for the most sensitive data classes (private message content, registration submissions). This adds a second key, separately held, for the highest-sensitivity prose.
- Key management: encryption keys live only on the production server with restrictive filesystem permissions. They are not stored in source control, log files, process listings, or backups. The platform owner maintains offline copies (password manager + physical safe) for recovery.
- Backups: daily, encrypted with a third independent key on the production server before being uploaded off-site. Off-site backups are stored in a separate Canadian-hosted, encrypted object store. An attacker would need to compromise both the production server and the off-site object store, and defeat multiple independent encryption keys, to obtain plaintext from cold storage.
- Network: the production database is bound to localhost only and is not directly reachable from the public internet. The host firewall denies inbound traffic to the database port from any source.
- Access: role-based access controls within each team environment. Administrative access is server-enforced and logged.
- Authentication: passwords stored as Argon2id one-way hashes (modern memory-hard algorithm). Login attempts are rate-limited and logged.
- Login activity is logged for security monitoring.
- Privacy breach notification process consistent with Canadian law.
- Biannual internal security reviews scheduled (first review: November 2026).
- Detailed security summary available at all24.ca/info/security and on request for institutional review.

Data architecture and residency

ALL24's architecture is designed around Canadian data residency for user account information.

Data at rest — Canada

User account data — names, email addresses, attestations, team memberships, chat messages, watch history, and login records — is stored at rest on **OVH** infrastructure in **Beauharnois, Quebec, Canada**. This data is subject to Canadian legal jurisdiction. The OVH Beauharnois data centre holds **ISO 27001, ISO 27017, ISO 27018, and SOC 1/2/3 (SSAE 18)** certifications.

Application processing — Canada

The ALL24 application server is hosted on the same Canadian infrastructure. User requests are processed within Canada, with data flowing between application and database over encrypted (TLS) connections. No persistent copy of user account data exists outside Canada.

Media storage — mixed regions (disclosed)

Team film and other coaching media is stored on **Cloudflare R2**, configured with an Eastern North America (ENAM) location preference. ENAM includes Canadian and US data centres. Cloudflare R2 does not currently offer a Canadian-only Jurisdictional Restriction option for this product (only EU and FedRAMP jurisdictions are available). Programs requiring strict Canadian-residency for media should contact us before adopting the platform.

Transient video processing — United States

AWS MediaConvert and **S3** transiently process video content in the United States during the encoding workflow. Transient files are automatically deleted within 48 hours. No persistent media storage occurs on AWS; this processing is solely the encoding pipeline.

Other supporting services

- **Google Firebase** delivers push notifications (US).
- **Stripe** processes payments under its own privacy practices (US). AMGI does not receive or store payment card data.

These providers operate under their own privacy practices and are listed in the Privacy Policy.

Frequently asked questions

Where is student data stored?

User account data — names, email addresses, attestations, team memberships, chat messages, watch history, and login records — is stored at rest on OVH infrastructure in Beauharnois, Quebec, Canada. This data is subject to Canadian legal jurisdiction. OVH's

Beauharnois facility holds ISO 27001, ISO 27017, ISO 27018, and SOC 1/2/3 (SSAE 18) certifications. The application server is hosted in the same Quebec facility.

Some supporting infrastructure is based in or routes through other regions: Cloudflare R2 stores team film with an Eastern North America location preference (which includes Canadian and US data centres); AWS MediaConvert and S3 transiently process video for under 48 hours; Firebase delivers push notifications; Stripe processes payments. All of this is disclosed in our Privacy Policy.

Is ALL24 PIPEDA compliant?

Yes. ALL24 is operated by an Ontario corporation and follows PIPEDA's principles of accountability, consent, limited collection, accuracy, safeguards, openness, individual access, and challenging compliance. The Privacy Policy describes our practices in detail. We have a designated Privacy Officer reachable at privacy@all24.ca.

How does ALL24 handle parental consent for students under 18?

Parental consent is obtained at the team level by the coach or team administrator, consistent with how other team apps and communication tools are typically introduced to students. At registration, students under 18 attest that they have parental or guardian permission. The Team Agreement places responsibility for ensuring those consents have been obtained on the team administrator. AMGI does not contact parents directly to verify consent. For school programs, we recommend that ALL24 be added to the existing parent communication or consent packet at the start of the season.

Can students under 13 use ALL24?

No. Registration requires attestation that the user is at least 13. The platform is not designed for under-13 users. A future parent-controlled account model is on the roadmap for younger users but is not yet implemented. Until then, programs serving players under 13 are not the platform's target audience.

Does ALL24 sell or share student data?

No. ALL24 does not sell user data. We do not share data with third parties for advertising, marketing, or any other commercial purpose. The only third parties with access to data are the infrastructure providers listed in the Privacy Policy, and they are bound by their own data processing agreements and may not use the data for their own purposes.

Are there ads on ALL24?

No. ALL24 is ad-free. There is no advertising in any part of the platform, and no third-party tracking or analytics tools are used.

What happens if a student or parent wants their data deleted?

The student can delete their account at any time from their account settings. A parent can ask the coach to remove the student from the team, or contact privacy@all24.ca directly. Account deletion includes a 30-day grace period in case of accidental deletion; after that, all personal information is permanently removed. Team-scoped data (chat, watch history) is stripped on a separate 14-day cycle when the student leaves the team voluntarily; on coach-initiated removal, access is revoked immediately and the data is stripped after a 48-hour reinstate window. De-identified usage analytics may be retained but contain no information that can be linked back to the individual.

Can students access a record of their data?

Yes. Every student can download a complete archive of their account from **Settings → Privacy → Download my data**. The archive is a ZIP file containing JSON-per-section data alongside a human-readable summary. It includes their account information, registration date, every attestation they made (with the verbatim text of every agreement they accepted at the time of acceptance, with timestamps), their login history, watch history, chat messages, team membership history, and references to any media (avatars, etc.) they uploaded. This implements PIPEDA's right of access.

How does ALL24 handle conduct issues like bullying or harassment?

Conduct issues are handled through a tiered process. Users can report misconduct in team chat or in direct messages through the platform. Reports go first to the team's coaches, who are the primary accountable parties for the conduct of users on their team. If a user accumulates five or more reports, or the matter is serious, it can be escalated to ALL24 administrators, who can review reported messages, suspend accounts, or in extreme cases suspend the team's access. Direct messages are private to the participants by default but are reviewable when reported, providing accountability without mass surveillance.

Are direct messages between users private?

DMs are private to the two participants — coaches cannot read DMs they are not part of, and other students cannot see them. DMs are text only — no image sharing. However, any user can report a DM for misconduct, and reported DMs are reviewable by ALL24 administrators as part of the conduct escalation process. This balances user privacy against the need for accountability in a youth-facing platform.

Does ALL24 require school IT integration or special network access?

No. ALL24 is a standard cloud-based web and mobile application accessed through any modern browser or via the mobile app. It does not require integration with school networks or installation of any software on school devices. There is no on-premises component. Single sign-on with school-managed identity providers (Google Workspace, Microsoft 365) is on the roadmap but not currently implemented.

What's the contracting model? Is this an enterprise contract?

ALL24 is licensed at the team level, not the district or school level. A football program purchases an annual subscription for the team and the coach manages the account. There is no district-wide contract required. Pricing is per-team, billed annually by invoice. This is intentionally lightweight — it allows individual programs to adopt ALL24 without triggering the full procurement process most boards apply to district-wide vendor relationships.

Is ALL24 added to vendor-of-record lists for school boards?

Not at this time. ALL24 is in early adopter phase as of May 2026 and operates at a scale that does not yet warrant vendor-of-record relationships with major school boards. Programs that require this designation should contact us directly at sales@all24.ca to discuss the path forward. Most early adopters have onboarded through their team's athletic budget rather than through district-level procurement.

What is ALL24's insurance coverage?

Ascension Media Group Inc. carries Commercial General Liability and Professional Liability (Errors & Omissions) insurance. Certificates of insurance are available on request. Coverage limits and details can be provided to procurement officers as part of any institutional review.

Does ALL24 have a Data Processing Agreement (DPA) available?

Yes. A standard DPA template (v1.1) is available to institutional reviewers on request. Email legal@all24.ca with your role and institution and we will send a one-time secure access link. The DPA describes the controller/processor relationship, sub-processor list (Schedule A), security measures, breach notification, retention, and audit rights.

What happens to team data if our subscription ends?

Team data is retained for 12 months following non-renewal or termination, allowing for account reinstatement. The team can request earlier deletion at any time during this window by contacting support@all24.ca. After 12 months, all team content and associated account data is permanently deleted.

Can a school audit our team's use of ALL24?

Yes, with the cooperation of the team administrator. The team's coach can request per-player compliance records (showing each user's registration, attestations, and accepted agreements) from privacy@all24.ca. Schools that want a deeper review (e.g., Privacy Impact Assessment, security questionnaire) can contact privacy@all24.ca and we will respond to reasonable requests.

Is ALL24 compliant with [specific provincial education privacy framework]?

ALL24 is designed to be PIPEDA-compliant and to align with provincial frameworks such as MFIPPA in Ontario, Quebec Law 25, BC PIPA / FOIPPA, Alberta PIPA / FOIP, and ATIPPA elsewhere. Specific provincial education privacy frameworks place obligations primarily on the school board itself rather than on third-party tools, but we are happy to work with school IT and privacy officers to address specific requirements. Note: BC's "Canada-only storage" requirement was repealed in 2021 (Bill 22) and replaced with an "adequate protection" standard. Contact privacy@all24.ca with your specific compliance question.

How ALL24 compares to common tools

Schools already use cloud-based tools that handle far more sensitive student data than ALL24. To put ALL24 in context:

vs. Google Workspace for Education or Microsoft 365 Education: Those platforms hold student documents, emails, calendar information, and academic content. ALL24 holds names, emails, and football-specific data only.

vs. Hudl, the dominant US-based football platform: Hudl is operated from the United States with US-based infrastructure for both data storage and processing. ALL24 is Canadian-operated, with user account data stored in Quebec, Canada, designed specifically for Canadian football, and collects less data overall.

vs. TeamSnap, GroupMe, or other team communication apps: Those platforms typically collect phone numbers and may share data with third-party advertisers. ALL24 collects no phone numbers and runs no advertising.

This comparison is provided for context only. Each platform has its own privacy posture and should be evaluated on its own terms.

How to proceed

If a single team in your school wants to use ALL24

This is the typical path for most early adopters. The team's coach or athletic department signs up directly through all24.ca. The coach manages the team and is the accountable party. School administrators may want to verify that the coach has informed parents and that the program is consistent with school policies on third-party communication tools.

If your athletic department wants a program-wide rollout

Contact sales@all24.ca to discuss program-wide arrangements. We can support multi-team configurations under a single athletic department, with consolidated billing and unified administrative oversight.

If your school board wants to formally evaluate ALL24

Contact privacy@all24.ca and legal@all24.ca. We will provide the legal documents, security summary, certificate of insurance, and DPA (when available), and respond to any specific privacy or compliance questions. We are a small Canadian company and we engage these reviews directly.

Contacts

- General: support@all24.ca
 - Privacy Officer: privacy@all24.ca
 - Legal and contracts: legal@all24.ca
 - Sales and program-wide arrangements: sales@all24.ca
 - Mailing address: Ascension Media Group Inc., 114 Gemini Drive, Hamilton, ON L9C 6C4
-

Privacy: privacy@all24.ca · Legal: legal@all24.ca

all24.ca · Ascension Media Group Inc. · Hamilton, Ontario

This guide is provided for informational purposes. The ALL24 [Terms of Service](#), [Privacy Policy](#), and [Team Agreement](#) are the legally binding documents.

Document version: May 2026 · v1.4