

School Board Privacy Package — The Self-Agency Project

Vendor: Elevation650 (Alberta, Canada) · Privacy Officer: Andrew Kiedyk · admin@elevation650.com · +1 780-228-5325 · selfagency.ca/privacy-compliance. Each row states a legal requirement with its full reference, followed by how we address it. Supports your Privacy Impact Assessment and vendor review under Alberta's Protection of Privacy Act and your Privacy Management Program.

Alberta PIPA — governs Elevation650's own handling of personal information

Legal requirement (with full reference)	How The Self-Agency Project addresses it
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · ss. 5–6 — Accountability and policies</i> Organizations must designate an individual accountable for compliance and make their privacy policies and practices available.	A designated Privacy Officer (Andrew Kiedyk, admin@elevation650.com) is accountable for compliance. Our privacy policies, including our use of service providers outside Canada, are published at selfagency.ca/privacy-compliance and available to anyone on request.
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · ss. 7–8 & 13 — Consent and notification</i> Consent is required to collect, use or disclose personal information, and individuals must be told the purposes of collection.	Public customers consent at booking, purchase, or account creation, and we state the purposes of collection at that point. School-seat student information is collected under the authority of the contracting school board (see POPA row).
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · s. 13.1 — Service providers outside Canada</i> Organizations using a service provider outside Canada must notify individuals and name a contact who can answer questions about foreign handling.	We disclose every provider and its country (see the subprocessor table) and name a contact for questions about foreign handling: admin@elevation650.com.
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · ss. 24–25 — Access and correction</i> Individuals have a right to request access to, and correction of, their personal information, with a response within statutory timelines.	Individuals (or the board on their behalf) may request a copy or correction via admin@elevation650.com; we respond within 45 days as the Act requires.
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · s. 34 — Safeguards</i> Organizations must protect personal information with reasonable security arrangements against unauthorized access, use, disclosure, copying, modification or destruction.	All traffic is encrypted in transit (TLS). Passwords are stored only as salted bcrypt hashes. Access is role-based (administrator / teacher / student) and limited to authorized staff. Administrative actions on sensitive data are audit-logged. The database is encrypted at rest and not publicly reachable.
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · s. 34.1 — Breach notification</i> Organizations must notify the Information and Privacy Commissioner (OIPC) of any breach creating a real risk of significant harm, without unreasonable delay.	Documented incident response: contain, assess, notify the affected school board without unreasonable delay (target: within 72 hours of discovery), notify the OIPC where the breach creates a real risk of significant harm, and notify affected individuals.
<i>Personal Information Protection Act (PIPA), SA 2003, c P-6.5 (Alberta) · s. 35 — Retention</i> Personal information may be retained only as long as reasonably required for legal or business purposes, then destroyed or anonymized.	Published retention schedule: student learning data deleted within 60 days of contract end or on the board's request, with written confirmation available; bookings/messages up to 2 years; signed legal records for limitation periods; financial records 7 years (CRA).

Alberta POPA (formerly FOIP) — governs school boards; binds Elevation650 as their service provider

Legal requirement (with full reference)	How The Self-Agency Project addresses it
<i>Protection of Privacy Act (POPA), SA 2024 (Alberta) — replaced FOIP for public bodies, June 2025 · Service-provider duties to public bodies</i> A service provider to a public body may collect, use and disclose personal information only to perform the contracted service, must safeguard it, must report privacy incidents, and must return or destroy it when the contract ends.	Student data is collected and used on behalf of, and under the authority of, the contracting school board, solely to deliver the purchased training — never for advertising, profiling, resale, product analytics unrelated to the service, or AI training. We sign board data-sharing / service agreements, notify boards of privacy incidents within 72 hours, limit access to authorized staff, use no subcontractors beyond the disclosed providers, and return or securely destroy student data at contract end or on request. We support board Privacy Impact Assessments with this package.

Canada PIPEDA — applies to personal information crossing provincial or national borders

Legal requirement (with full reference)	How The Self-Agency Project addresses it
<i>Personal Information Protection and Electronic Documents Act (PIPEDA), SC 2000, c 5 (Canada) · Application and Schedule 1 fair-information principles</i> Alberta's PIPA is declared substantially similar to PIPEDA, so PIPA governs our handling of personal information within Alberta. PIPEDA continues to apply to personal information that crosses provincial or national borders in the course of commercial activity, requiring accountability, safeguards, openness and limits on use.	Cross-border flows exist only through our disclosed U.S. service providers (see table). Each receives the minimum needed for its function, is bound by terms limiting use to supplying the service, and is covered by the same safeguards, breach-response and disclosure practices listed above (PIPA s. 13.1 disclosure; PIPEDA accountability and safeguards principles).

Canada CASL — commercial electronic messages (email & text)

Legal requirement (with full reference)	How The Self-Agency Project addresses it
<i>Canada's Anti-Spam Legislation (CASL), SC 2010, c 23 · ss. 6–11 — Consent, identification and unsubscribe</i> Commercial electronic messages require the recipient's consent, must identify the sender, and must include a working unsubscribe mechanism.	Promotional texts (e.g., discount codes) are sent only to existing customers or people who requested them, with consent recorded at the time of sending. Every message identifies us and supports STOP to opt out. Transactional messages (bookings, receipts, course access) are sent as part of the service.

Service providers (subprocessors) — PIPA s. 13.1 / PIPEDA disclosure

Provider	Purpose	Country
Stripe	Payment processing	United States
Twilio	Text messages (sending & receiving)	United States
Resend	Transactional email	United States
Google	Business calendar scheduling only	United States
Secure cloud hosting	App hosting & encrypted database	United States

Notes for reviewers

- What we collect about students: name, email address, and course progress (lessons completed, quiz results, certificates). Nothing else is required. Payment information is handled by the board, not collected from students.
- Agreements: we will sign the board's data-sharing / service agreement, complete security questionnaires, and support PIA inquiries. Parent/guardian consent for participation is managed by the school under its own policies.

- This document is provided for information and procurement-review purposes and is not legal advice. The current version is always available at selfagency.ca/privacy-compliance.

Privacy Officer: Andrew Kiedyk · Elevation650 · admin@elevation650.com · +1 780-228-5325 · selfagency.ca/privacy-compliance