



POWERED BY INTELLIDU EDUCATION · CANADA

DOCUMENT 01 OF 13 · PUBLIC WEBSITE PAGE

Privacy Policy

How SkillShift+ collects, uses, discloses, safeguards and retains personal information

Platform	SkillShift+ (skillshift.ca)
Operator	Intelliedu Canada Inc. (registered spelling to be confirmed against Articles of Incorporation)
Registered address	135 Hillcrest Avenue, Mississauga, Ontario, Canada L5B 4B1
Privacy Officer	Dr. Chandan Singh
Contact	info@skillshift.ca
File name	01SkillShiftPrivacy_Policy.docx
Version	1.0 — Draft
Effective date	July 28, 2026
Next scheduled review	July 28, 2027, or upon material change

© 2026 Intelliedu Canada Inc. · All rights reserved. · Confidential draft — not for distribution outside the SkillShift+ project team and its legal advisers.

Table of contents

This table of contents is a live Microsoft Word field. If it appears blank, click anywhere in it and press F9 (or Ctrl+A then F9) to generate the entries and page numbers.

1. Introduction and scope

SkillShift+ is a Canadian education, career-readiness and workforce-development platform operated by **Intelliedu Canada Inc.** ("Intelliedu", "we", "us" or "our"), a company with its registered office at 135 Hillcrest Avenue, Mississauga, Ontario, Canada L5B 4B1. SkillShift+ is presented with the attribution "Powered by IntelliDu Education".

This Privacy Policy (the "**Policy**") explains what personal information we collect when you use SkillShift+, why we collect it, how we use and disclose it, how long we keep it, how we protect it, and the choices and rights available to you. It is written to reflect the requirements of the *Personal Information Protection and Electronic Documents Act* (Canada) ("**PIPEDA**") and its ten fair information principles, together with Ontario and federal laws that apply to our activities.

This Policy applies to all of the following:

- the SkillShift+ website, user accounts and account settings;
- the SkillShift+ course catalogue, including the thirty-five (35) course categories and their approximately twelve to fifteen (12–15) modules per course;
- videos, study materials and downloadable learning resources;
- quizzes, module assessments and AI-supported simulations;
- the Career Readiness Assessment (free tier and paid report);
- personalized Career Readiness Reports;
- the AI Interview Coach, including audio and video practice sessions where enabled;
- the Resume Builder;
- the Skill Passport and its 0–1000 workforce-readiness score;
- the Licensing Navigator;
- Certificates of Completion and digital badges;
- payments, subscriptions, credits and billing;
- the Organization and Administrator Portal, where an organization has been granted access;
- customer support and other communications with us; and
- any mobile application or future version of the platform that links to this Policy.

This Policy does not apply to third-party websites, employers, regulators, educational institutions or services that we link to or that you choose to share your information with. Those organizations have their own privacy practices, and we encourage you to review them.

By creating an account you acknowledge that you have read this Policy. Acknowledgement of this Policy is recorded separately from your acceptance of the Terms of Use and separately from any consent you give to artificial intelligence ("**AI**") processing, interview recording or marketing communications.

2. Defined terms

Term	Meaning
Account	The registered user account through which a User accesses SkillShift+.
AI Features	Platform features that send information to a third-party AI service for processing, including Career Reports, the AI Interview Coach, Resume assistance, simulations, career recommendations, Skill Passport insights and course-support tools.
Career Report	The personalized Career Readiness Report generated for a User, including the paid report offered at CAD 39.
Consent Record	The database record evidencing a specific permission granted or refused by a User, including its type, version, timestamp and method.
De-identified Information	Information from which direct and indirect identifiers have been removed such that an individual cannot reasonably be re-identified in the circumstances, and which we do not attempt to re-identify.
Personal Information	Information about an identifiable individual, as that term is used in PIPEDA. It does not include the business contact information of an individual used solely for business communication, to the extent permitted by law.
Platform	The SkillShift+ platform in all of the forms described in section 1.
Privacy Officer	The individual accountable for Intelliedu's compliance with this Policy, identified in section 3.
Service Provider	A third party engaged by Intelliedu to process information on our behalf and under our instructions, as listed in section 9.
Skill Passport	The dynamic 0–1000 workforce-readiness score and supporting evidence record maintained for a User.
User	An individual who creates an Account or otherwise uses the Platform. "You" and "your" refer to a User.

3. Accountability and the Privacy Officer

Intelliedu Canada Inc. is accountable for the personal information under its control, including information transferred to a Service Provider for processing. We have designated a Privacy Officer who is responsible for our compliance with this Policy and with applicable privacy legislation.

Privacy Officer	Dr. Chandan Singh
Organization	Intelliedu Canada Inc.
Address	135 Hillcrest Avenue, Mississauga, Ontario, Canada L5B 4B1
Email	info@skillshift.ca

The Privacy Officer is responsible for responding to access, correction and deletion requests, maintaining our privacy documentation, overseeing the vendor register, managing privacy incidents, and reviewing this Policy at least annually.

4. Personal information we collect

We collect only the personal information that is reasonably necessary for the purposes identified in section 6. The categories below describe what may be collected; what is actually collected for any individual User depends on which features that User chooses to use. Many categories are optional, and optional fields are identified as such at the point of collection.

4.1 Account and identity information

- name;
- email address;
- telephone number, where provided;
- login credentials, including a password stored in hashed form, and session identifiers;
- social-login identifiers where social login is enabled and used (see section 5);
- age-confirmation information (see section 8).

4.2 Profile, career and eligibility information

- country, province or territory of residence, and city where provided;
- preferred occupation, job title and National Occupational Classification ("NOC") preference;
- education, credentials and qualifications;
- work experience, including employers, duties and durations where you enter them;
- language-test results and other skills information;
- licensing and regulatory interests used by the Licensing Navigator;
- immigration status, only where you voluntarily provide it;
- financial-capacity information, only where you voluntarily provide it for the paid Career Readiness Report;
- résumé content and uploaded documents.

LEGAL REVIEW NOTE

Immigration status and, in some contexts, information capable of revealing health or ethnic origin may be treated as sensitive personal information attracting a higher standard of consent and safeguarding.

SkillShift+ therefore collects immigration status only on an optional basis, explains why it is being requested at the point of collection, and does not make it a condition of using the Platform's core learning features.

4.3 Learning and assessment information

- course and module enrolment, progress, completion status and course locking or unlocking state;
- quiz answers, scores and attempt history;

- simulation inputs, responses and results;
- Career Readiness Assessment answers;
- Career Reports generated for you;
- Certificates of Completion and digital badges issued to you;
- Skill Passport inputs, evidence sources, points awarded and score history;
- Resume Builder content;
- employer or organization feedback, where an organization has been granted access and provides it.

4.4 AI Interview Coach information

- interview audio recordings, where you consent to audio recording;
- interview video recordings, where video practice is enabled and you consent to video recording;
- transcripts generated from those recordings;
- your typed or spoken answers, question-by-question scoring, AI feedback and improvement recommendations;
- credit balances, session counts and usage history.

4.5 AI interaction information

- prompts and inputs that you submit to AI Features;
- outputs returned to you;
- your ratings, corrections or feedback on AI outputs;
- technical metadata such as feature name, model identifier, timestamp and token or usage counts.

4.6 Payment and subscription information

- subscription plan, status, renewal date and cancellation status;
- purchase records, transaction identifiers, amounts, currency, receipts and invoices;
- refund and chargeback records;
- billing contact information;
- credit balances and expiry dates for one-time and monthly interview credits.

We do not normally store full payment card numbers. Card details are collected and processed by Stripe. See section 11.

4.7 Technical, security and support information

- IP address, browser type, device type, operating system and approximate region derived from IP address;
- authentication events, security logs, rate-limiting events and error logs;
- cookie and similar-technology identifiers, as described in the Cookie Policy;
- Consent Records, including grants, refusals, notice versions and withdrawals;
- support tickets, emails and other communications with us, including attachments you send.

Limiting collection. We do not intentionally collect more personal information than is reasonably necessary for the identified purpose. We ask you not to submit sensitive personal information — including health

information, government identification numbers, Social Insurance Numbers or financial account numbers — into free-text fields, résumé uploads, AI prompts or interview answers where it is not required.

5. Where information comes from

We collect personal information from the following sources:

Source	What we receive
Directly from you	Registration details, profile and career information, assessment answers, uploads, résumé content, AI prompts, interview responses, support messages and consent choices.
Your activity on the Platform	Course enrolment and progress, quiz and simulation results, certificate issuance, Skill Passport events and feature usage.
Social login (Google or Facebook), where enabled	Basic profile identifiers such as name, email address and account identifier, in accordance with the permissions you approve with that provider. Facebook login is disabled unless and until it has been fully configured and tested.
Stripe	Payment status, transaction identifiers, subscription state, refund status and limited billing contact information. Stripe does not provide us with full card numbers.
Service Providers	Operational information necessary to deliver, secure and support the Platform, such as delivery status for transactional email and system error information.
Security and operational logs	Authentication events, IP addresses, device information and abuse or rate-limiting signals generated automatically by our infrastructure.
Organizations, where applicable	Where you use SkillShift+ under an organization or employer account, that organization may provide enrolment information and may supply employer feedback that contributes to your Skill Passport.

6. Why we collect, use and disclose personal information

We identify the purposes for which personal information is collected at or before the time of collection. We use personal information for the following purposes:

Purpose	Typical information used
Creating and authenticating your Account	Name, email address, credentials, session and device information.
Delivering courses, modules, videos and study materials	Account identifiers, enrolment and progress records.
Tracking progress and unlocking course content	Module completion, quiz and simulation results.
Scoring quizzes and simulations	Answers, attempt history and scoring rules.
Generating Certificates of Completion and digital badges	Name, course and completion records, certificate identifier.

Purpose	Typical information used
Calculating and maintaining the Skill Passport score	Course, quiz, simulation, certificate, interview, experience, licensing, engagement, verification and employer-feedback events.
Generating Career Readiness Reports	Assessment answers, profile, education, experience, language, province, status and, where provided, financial information.
Operating the Licensing Navigator	Occupation, NOC preference, province and credential information.
Building and storing résumés	Résumé content supplied by you.
Providing AI Interview Coach sessions and feedback	Questions, your answers, audio or video where consented, transcripts and scoring.
Making personalized course and career recommendations	Profile, assessment and progress information.
Processing payments, subscriptions, credits and refunds	Billing contact information and Stripe transaction records.
Preventing fraud, duplicate point awards and account abuse	Security logs, device and IP information, Skill Passport audit trail.
Providing technical and customer support	Support communications and relevant account records.
Monitoring, securing and maintaining the Platform	Security, error and performance logs.
Meeting legal, regulatory, tax and accounting obligations	Payment, invoice, consent and incident records.
Improving the Platform using aggregated or De-identified Information	Usage statistics that do not identify individuals.
Sending marketing communications	Name and email address — used for this purpose only where you have given separate marketing consent.

If we propose to use personal information for a purpose that is not identified in this Policy and that is not permitted or required by law, we will identify that purpose and obtain your consent before doing so.

7. Artificial intelligence processing

Several SkillShift+ features rely on AI processing performed through the **OpenAI API**. This section explains that processing. A shorter, feature-level notice is presented before you first use an AI Feature; see the *AI Consent and Transparency Notice*.

7.1 Features that use AI

- Career Readiness Reports;
- AI Interview Coach, including question generation, scoring and feedback;
- Resume Builder assistance;

- module simulations;
- career and course recommendations;
- Skill Passport insights and narrative summaries;
- course-support tools such as explanation and practice aids.

7.2 What is sent, and why

Feature	Information transmitted for processing	Why it is transmitted
Career Report	Assessment answers and relevant profile fields (education, experience, language, province, status and occupation).	To produce an individualized readiness analysis and pathway narrative.
AI Interview Coach	Interview questions, your answers and, where audio or video practice is used and consented to, the transcript of your response.	To score answers and generate question-by-question feedback.
Resume Builder	Résumé sections you choose to have improved.	To suggest wording and structure.
Simulations	Your simulation inputs and the scenario context.	To evaluate responses and provide feedback.
Recommendations	Occupation preference, progress and assessment summary.	To suggest courses and next steps.
Skill Passport insights	Score components and evidence categories.	To generate a plain-language explanation of your score.

We are committed to transmitting only the information reasonably necessary for the relevant feature. Where a feature can operate on a summarized or partial record, we aim to send the summary rather than the full profile.

7.3 Training, retention and provider practices

- **SkillShift+ does not use customer personal information to train AI models.**
- **SkillShift+ will not opt in to any AI provider programme that would permit our customers' inputs or outputs to be used for model training.**
- OpenAI states that inputs and outputs submitted through its API are not used to train its models by default unless the customer explicitly opts in. We rely on that default and do not opt in.
- Standard API abuse-monitoring logs may nevertheless be retained by the provider for a limited period — currently stated by OpenAI as up to thirty (30) days — depending on the API feature and account controls in use. We do not represent that no copy of the information exists anywhere outside our systems.
- AI processing may occur on servers located outside Ontario and outside Canada. See section 10.

7.4 Our own retention of AI inputs and outputs

We retain AI inputs and outputs in accordance with the retention schedule in section 13. In summary: interview audio and video are retained for ninety (90) days unless deleted earlier; interview transcripts and AI

feedback are retained for twelve (12) months; and Career Reports, Skill Passport data and Resume Builder content are retained for the active period plus up to twenty-four (24) months.

7.5 Limitations of AI output

- AI output may be incomplete, inaccurate, outdated or inconsistent, and may reflect bias present in underlying data.
- AI output is informational and educational. It does not constitute legal, immigration, licensing, financial or employment advice.
- **AI does not make final employment, immigration, licensing or admission decisions on the Platform, and no such decision is made about you by automated means without the ability to obtain human review.**
- Scores, including AI-influenced components of the Skill Passport, are indicative and are not a determination of employability.
- You should verify important information — including licensing requirements, NOC classification and immigration criteria — with the responsible employer, regulator, institution or government authority before relying on it.

8. Consent

We obtain consent that is meaningful: consent given with a reasonable understanding of what is collected, who it is shared with, why, and what the reasonably foreseeable consequences are. Consent is obtained separately for materially different activities. **A single general checkbox covering everything is not used.**

8.1 Separate permissions

Permission	Nature	How it is obtained
Acceptance of the Terms of Use	Required to use the Platform.	Express, at registration.
Acknowledgement of this Privacy Policy	Required to use the Platform.	Express, at registration.
AI processing consent	Required for AI Features only.	Express, before first use of an AI Feature.
Interview audio or video recording consent	Required for recorded interview practice only.	Express and separate, before each recorded session.
Marketing communications consent	Optional.	Express opt-in, unchecked by default.
Public sharing of a certificate or Skill Passport	Optional.	Express opt-in per share action.
Social-login permission	Optional.	Granted through the social provider's permission screen.
Optional cookies	Optional.	Through the cookie banner and preference centre.

8.2 What we record

For each permission we record: the user identifier; the consent type; whether it was granted or refused; the version of the notice presented; the date and time; the method of collection; the withdrawal date where applicable; and, where appropriate for security and evidentiary purposes, the device or IP address associated with the action.

8.3 Withdrawing consent

You may withdraw an optional consent at any time, subject to legal or contractual restrictions and reasonable notice. Withdrawal is not retroactive: it does not affect processing already carried out lawfully. Withdrawing AI consent will disable AI Features, and withdrawing recording consent will disable recorded interview practice. Some withdrawals will limit or prevent your use of parts of the Platform, and we will tell you when that is the case before you confirm.

To withdraw consent, use the controls in your account settings where available, or email info@skillshift.ca.

8.4 Consent exceptions

In limited circumstances permitted by law, we may collect, use or disclose personal information without consent — for example, to investigate a breach of an agreement or a contravention of law, to prevent or detect fraud, where the information is publicly available as defined by regulation, in an emergency threatening life, health or security, or where required by a court order, subpoena, warrant or other lawful demand.

9. Minors

AGE REQUIREMENT

Users must be at least 16 years old. Users who have not reached the age of majority in their province or territory must obtain permission from a parent or legal guardian before purchasing services, uploading sensitive documents, recording interview audio or video, or using AI features that process personal information.

SkillShift+ is not directed at children under 16 and we do not knowingly collect personal information from them. If we become aware that we have collected personal information from a person under 16, we will delete it promptly, subject to any records we are required by law to retain.

At registration we ask you to confirm that you meet the minimum age. We ask for age confirmation rather than collecting a full date of birth where a full date of birth is not required for the feature you are using. If we later require a date of birth for a specific purpose, we will explain that purpose at the point of collection.

If you are a parent or guardian and believe that a person under 16 has created an Account, contact info@skillshift.ca and we will investigate.

10. Service Providers and disclosure

We do not sell personal information. We do not rent or trade personal information. We disclose personal information only as described in this section.

10.1 Service Providers

We engage the following categories of Service Provider to process information on our behalf. Each receives only the information reasonably needed to perform its service, and is required by contract to protect it and to use it only for the purposes we specify.

Service Provider	Role	Categories of information processed
Vercel	Application hosting and deployment	Request data, IP address, technical logs and content transiting the application layer.
Supabase	Database, storage and authentication	Account, profile, learning, assessment, Skill Passport, résumé, consent and uploaded file data.
Stripe	Payment processing	Billing contact information, payment card data (collected by Stripe directly), transaction and subscription records.
OpenAI	AI processing via API	Prompts, inputs and outputs for AI Features, as described in section 7.
GoDaddy	Domain registration and business email	Business email content and routing information.
Resend	Transactional email delivery, if retained in production	Recipient email address, message content and delivery status.
Error and security monitoring provider, if later added	Application error and security monitoring	Technical error and security event data. Any such provider will be added to this Policy and to our vendor register before use.

A detailed internal Vendor and Subprocessor Register is maintained by the Privacy Officer and updated whenever a provider is added, changed or removed.

10.2 Other disclosures

- **With your direction** — for example, where you choose to share a certificate, Skill Passport or résumé with an employer or third party.
- **To an organization account** — where you use SkillShift+ under an employer or organization licence, that organization may access enrolment, progress, completion and certificate information relating to your participation. The scope is disclosed to you at enrolment.
- **To professional advisers** — legal, accounting and audit advisers under duties of confidentiality.
- **To comply with law** — in response to a court order, subpoena, warrant, regulatory demand or other lawful requirement, or to establish, exercise or defend legal claims.
- **To protect safety and prevent harm** — where permitted or required by law, including to prevent or investigate fraud, abuse or a threat to the life, health or security of any person.
- **In a business transaction** — in connection with a proposed or completed merger, acquisition, financing or sale of assets, in accordance with the requirements of PIPEDA relating to business transactions, including confidentiality and use restrictions.

11. Processing outside Ontario and outside Canada

Our Service Providers may store or process personal information on servers located outside the Province of Ontario and outside Canada, including in the United States and other jurisdictions.

While personal information is located in another jurisdiction, it may be accessible to the courts, law enforcement and national security authorities of that jurisdiction under the laws applicable there, including through lawful access requests, regardless of the protections we have put in place by contract.

We remain accountable for personal information transferred to a Service Provider for processing, and we use contractual and other means to require a comparable level of protection while the information is being processed on our behalf.

LEGAL REVIEW NOTE

This Policy deliberately does **not** state that all information remains in Canada. Such a statement must not be added unless the exact data-residency configuration of Vercel, Supabase, Stripe, OpenAI, GoDaddy and Resend has been verified in writing and is enforced in the production configuration.

If Canadian or regional data residency is later configured and verified, this section should be revised and the Vendor Register updated to record the verified region for each provider.

12. Payments

- Card payments are processed by **Stripe**. Card details are submitted to Stripe and are not normally stored on our systems.
- We retain transaction identifiers, amounts, currency, receipts, invoices, subscription status, refund status, credit balances and billing contact information.
- Stripe processes payment information as an independent controller for certain purposes, including fraud prevention and legal compliance, and its own privacy terms apply in addition to this Policy.
- Financial records are retained for seven (7) years, as explained in section 13.

Refund, cancellation, subscription and access rules are set out in the *Refund, Cancellation, Subscription and Access Policy*.

13. Retention

We retain personal information only as long as necessary to fulfil the purposes for which it was collected, or as required by law. We do not apply a single blanket retention period to all information. The following schedule applies:

Information	Retention period
Active account profile	For as long as the Account remains active.
Profile information after account closure	Up to 24 months after closure.
Course progress and assessment records	Active period plus up to 24 months.

Information	Retention period
Skill Passport data and Resume Builder content	Active period plus up to 24 months.
Career Reports	Active period plus up to 24 months.
Interview audio and video recordings	90 days, unless deleted earlier by the User.
Interview transcripts and AI feedback	12 months.
Support records	24 months after the matter is resolved.
Security logs	12 months.
Consent and withdrawal records	7 years.
Payment, invoice and tax records	7 years.
Certificate verification record	7 years, using the minimum data necessary to verify authenticity.
Backups containing deleted account data	Removed through normal backup rotation within 90 days.
Properly de-identified statistics	May be retained longer where re-identification is not reasonably possible.

The seven-year periods reflect the Canada Revenue Agency requirement that business records generally be kept for six years from the end of the relevant tax year, with a buffer. **That financial-records requirement does not justify retaining course, interview, assessment or résumé information for seven years**, and we do not do so.

When a retention period expires, information is securely deleted or irreversibly de-identified. Where information is subject to a legal hold, it is retained until the hold is lifted.

14. Your privacy rights

Subject to the exceptions permitted by law, you may make the following requests:

Right	What you can ask for
Access	Confirmation of whether we hold personal information about you, an account of its use and disclosure, and access to the information itself.
Correction	Correction of inaccurate or incomplete personal information.
Export	A copy of your account data in a commonly used, machine-readable format where reasonably practicable.
Deletion	Deletion or anonymization of personal information that we are not legally required to retain (see section 15).
Withdrawal of consent	Withdrawal of an optional consent, including AI, recording, marketing or public-sharing consent.
Marketing opt-out	Removal from marketing communications, without affecting transactional messages.

Right	What you can ask for
Information about disclosure	An account of the third parties to which your personal information has been disclosed.
Explanation of AI processing	An explanation of what information an AI Feature used, and the ability to request human review of a result that materially affects you.

Requests should be sent to info@skillshift.ca, addressed to the Privacy Officer. We may need to verify your identity before acting on a request, and we will use the least intrusive verification method reasonably available.

Under PIPEDA we will respond to an access request within thirty (30) calendar days of receipt, subject to the limited extensions permitted by law. Where an extension applies, we will notify you within the original thirty-day period, explain the reason and tell you when to expect a response. Where we refuse a request in whole or in part, we will explain why and tell you how to complain.

Access may be limited or refused where the information is subject to solicitor-client privilege, would reveal personal information about another individual, would compromise an investigation, or where another statutory exception applies. Where possible, we will sever the exempt material and provide the remainder.

15. Account deletion

You may ask us to close your Account and delete your information. The process is as follows:

- 1. Where to request.** A self-service deletion control in account Settings is an implementation requirement and will be described here as available only once it functions in production. Until then, deletion may be requested by email to info@skillshift.ca.
- 2. Identity verification.** We will verify that the request comes from the Account holder.
- 3. Active subscriptions.** Any active subscription must be cancelled or will be cancelled as part of the process. Deletion does not by itself generate a refund; refunds are governed by the Refund Policy.
- 4. What is deleted.** Personal information that we are not legally required to retain is deleted or irreversibly anonymized. This includes profile data, course progress, assessment answers, Career Reports, Skill Passport data, résumé content, interview media and transcripts, and AI inputs and outputs.
- 5. What is retained.** Payment, invoice and tax records, consent and withdrawal records, certificate verification records and records required for legal, security or fraud-prevention purposes are retained for the periods in section 13.
- 6. Backups.** Deleted information may persist in encrypted backups until those backups rotate out, normally within ninety (90) days.
- 7. Confirmation.** We will confirm completion by email.

16. Safeguards

We protect personal information with safeguards appropriate to its sensitivity, including:

- encryption of information in transit using industry-standard transport encryption;
- password hashing and secure credential handling through our authentication provider;

- role-based access controls and the principle of least privilege;
- restriction of staff and contractor access to those who need it for their duties;
- storage of secrets and API keys in environment variables rather than in source code;
- database backups and tested restore procedures;
- audit logging of administrative actions and Skill Passport point adjustments;
- rate limiting and abuse detection on authentication and API endpoints;
- file-type and file-size restrictions on uploads;
- reliance on the payment-provider safeguards maintained by Stripe for card data; and
- a documented privacy-incident response process.

No method of transmission or storage is completely secure, and we do not represent that the Platform is "100% secure." We work to maintain reasonable safeguards and to improve them over time. You are responsible for keeping your password confidential and for notifying us promptly of any suspected unauthorized use of your Account.

17. Privacy breaches

We maintain a documented privacy-incident process covering identification, containment, assessment, notification and remediation. If we suspect a breach of security safeguards, we investigate promptly, take steps to contain it and assess the risk to affected individuals.

PIPEDA requires organizations to keep a record of every breach of security safeguards, whether or not it is reportable. Where a breach creates a **real risk of significant harm** to an individual, we will report it to the Office of the Privacy Commissioner of Canada and notify affected individuals as soon as feasible, and will notify any other organization or government institution that may be able to reduce the risk of harm.

Notification to individuals will describe the circumstances of the breach, when it occurred, the personal information involved, the steps we have taken, the steps you can take to reduce risk, and how to contact us.

18. Email and marketing communications

18.1 Transactional messages

We send messages necessary to operate your Account and deliver the services you have requested. **These are not marketing messages and continue for as long as your Account is active**, including:

- account verification and password-reset messages;
- purchase receipts, invoices and subscription notices;
- course, enrolment, certificate and assessment notifications;
- security alerts and important service notices;
- responses to your support enquiries.

18.2 Marketing messages

Marketing messages — promotions, new-course announcements, offers and newsletters — are sent **only where you have given separate, express marketing consent**. The marketing checkbox is unchecked by default and is not bundled with Terms acceptance or Privacy Policy acknowledgement.

Every marketing message identifies Intelliedu Canada Inc. as the sender, provides our mailing address and contact information, and includes a working unsubscribe mechanism. **Canada's Anti-Spam Legislation requires unsubscribe requests to be given effect without delay and in any event within ten (10) business days**, and we do not require you to take any further step to have your request honoured. Unsubscribing from marketing does not stop transactional messages.

19. Cookies

We use cookies and similar technologies for authentication, security, preferences and payments. Strictly necessary cookies are used without consent because the Platform cannot function without them. Optional cookies are used only with your permission, through the cookie banner and preference centre. Analytics and advertising cookies are **not currently used**. Full details are in the *Cookie Policy*.

20. Changes to this Policy

We review this Policy at least annually. We may update it to reflect changes in our services, our Service Providers, or the law. The effective date and last-updated date appear on this document and on the published page.

Where a change is **material** — for example, a new category of personal information, a new purpose, a new Service Provider that receives personal information, or a change in AI processing — we will provide notice before the change takes effect, through the Platform or by email, and **will obtain fresh consent where the law requires it**. Continued use of the Platform after a non-material change takes effect indicates acceptance of the updated Policy.

Previous versions of this Policy are retained and are available on request.

21. Complaints

If you have a question or concern about our handling of your personal information, please contact the Privacy Officer first. We will acknowledge your complaint, investigate it, and inform you of the outcome and of any corrective action taken.

If you are not satisfied with our response, you may contact:

Office of the Privacy Commissioner of Canada	30 Victoria Street, Gatineau, Quebec K1A 1H3 · priv.gc.ca · Toll free: 1-800-282-1376
Other authorities	You may also contact the privacy regulator in your province or territory where one has jurisdiction over the matter.

Contact information

Questions, requests and complaints relating to this document may be directed to:

Operator	Intelliedu Canada Inc. (operating the SkillShift+ platform)
Attention	Dr. Chandan Singh, Privacy Officer
Address	135 Hillcrest Avenue, Mississauga, Ontario, Canada L5B 4B1
Email	info@skillshift.ca
Website	skillshift.ca
Effective date	July 28, 2026
Last updated	July 28, 2026
Version	1.0 — Draft for Canadian Legal Review