

Privacy Policy

Last Updated: September 19, 2025

LearnQuest and our subsidiaries and affiliates (“LQ,” “we,” “our,” or “us”) respect your privacy and are committed to protecting your personal information. This Privacy Policy explains how we collect, use, share, and safeguard information; describes your rights and choices; and details our compliance with the EU General Data Protection Regulation (GDPR), UK GDPR, California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), Children’s Online Privacy Protection Act and Rule (COPPA/COPPA 2.0), Health Insurance Portability and Accountability Act (HIPAA), and other global data protection laws.

1. Information We Collect

1.1 Directly from You

- When you register for an account, enroll in training, complete forms, make purchases, or communicate with us.
- Includes identifiers (name, email, phone number), credentials, payment details, and communications content.

1.2 Automatically Through Technology (Cookies & Tracking)

When you visit our sites or use our services, we automatically collect certain technical and usage data through cookies, pixels, scripts, and similar technologies. These include:

- Device and browser data (type, operating system, IP address, device ID)
- Usage data (pages visited, time on site, links clicked, training modules accessed)
- Cookie categories:
 - Strictly Necessary: Required for core functionality (login, security, cart).
 - Performance & Analytics: Collect usage statistics to improve services.
 - Marketing & Personalization: Enable targeted advertising and track ad effectiveness.

We manage cookies via a Consent Management Platform. You may adjust preferences at any time through the Cookie Settings link on every page.

1.3 From Third-Party Sources

We may receive information about you from trusted third parties, including:

- Service providers – e.g., payment confirmations from payment processors, fraud prevention checks, hosting providers

- Business partners – e.g., certification status and training completion records from accreditation partners, course enrollment data from training providers
- Marketing and analytics platforms – e.g., lead capture forms, advertising conversion data, event registrations
- Publicly available sources – e.g., professional profiles, company directories, industry databases

This data is used only for legitimate business purposes such as fulfilling transactions, validating credentials, improving services, and ensuring regulatory compliance.

1.4 Combination of Data

Where permitted, we may combine personal and non-personal data to improve accuracy, security, and personalization.

2. Legal Bases for Processing (GDPR Article 6)

We process personal data only when one or more of the following apply:

- Consent: You have given clear, affirmative consent for specific purposes.
- Contract: Necessary to perform or enter into a contract with you.
- Legal Obligation: Required to comply with laws or regulations.
- Legitimate Interests: Necessary for our legitimate interests, provided your rights do not override those interests. We document our Legitimate Interests Assessments (LIAs) upon request.

Purpose	Data Collected	Legal Basis
Payments and transactions	Identifiers, payment details	Contract
Account creation and management	Identifiers, credentials	Contract
Marketing communications	Identifiers, usage data	Consent
Service improvement & analytics	Technical data, cookies	Legitimate Interests
Compliance with legal obligations	Payment records, certification records	Legal Obligation
Fraud prevention & security	Technical data, account activity	Legitimate Interests / Legal Obligation

Third-party data integration (e.g., enriching profiles with publicly available/provided data)	Professional information, identifiers, and publicly available details	Legitimate Interests (documented via Legitimate Interests Assessment – LIA)
---	---	---

3. Cookies, Consent & Tracking

3.1 Cookie Categories

- Strictly Necessary: Required for core functionality; cannot be disabled.
- Performance & Analytics: Require consent to collect usage data.
- Marketing & Personalization: Require consent to deliver targeted content and ads.

3.2 Consent Management & Google Consent Mode

We use a Consent Management Platform to obtain your explicit, informed consent before setting any non-essential cookies. Until you provide consent, analytics and advertising tags are held back via Google Consent Mode v2 (signals include ad_storage, analytics_storage, ad_user_data, ad_personalization). You can change or withdraw consent at any time through the Cookie Settings link available on every page.

3.3 Third-Party Tags

We use the following third-party tags and services:

- Google Analytics 4 and Conversion Linker (analytics and conversion measurement)
- Google Ads Remarketing and Conversion Tracking (advertising and attribution)
- LinkedIn Insight Tag (advertising and conversion measurement)
- YouTube embeds (video playback and analytics)
- HubSpot forms (lead capture)
- Google reCAPTCHA (bot detection and security)

These providers may process online identifiers (including IP addresses), device information, page URLs, referrers, and event metadata. Transfers outside your jurisdiction are protected by Standard Contractual Clauses with Transfer Impact Assessments and supplemental safeguards per Schrems II guidance.

4. Sharing and Disclosure

4.1 Service Providers

We share data with third-party processors under Data Processing Agreements that enforce GDPR- and CCPA/CPRA-compliant safeguards. Categories include payment processors, IT hosting, analytics, event management, marketing platforms, and security services.

4.2 Cross-Context Behavioral Advertising (CPRA)

For California residents, we may “share” personal information for cross-context behavioral advertising via platforms such as Google Ads and LinkedIn to measure conversions and deliver relevant ads. We honor Global Privacy Control (GPC) signals as valid opt-out requests.

4.3 Legal Requirements

We may disclose personal data to comply with legal obligations, respond to lawful requests, or protect rights, property, or safety.

4.4 No Sale of Personal Information

We do not sell personal data.

However, under the California Privacy Rights Act (CPRA), certain uses of data for cross-context behavioral advertising (for example, using Google Ads or LinkedIn Insight Tag) are classified as “sharing.”

California residents may therefore exercise their right to opt out of such “sharing” by:

- Clicking the “**Do Not Sell or Share My Info**” link in the site footer,
- Sending an email request to Privacy.Compliance@learnquest.com, or
- Using a browser that sends a Global Privacy Control (GPC) signal, which we honor automatically.

This ensures compliance with CPRA while reaffirming our position that LearnQuest does not engage in the sale of personal data.

5. International Data Transfers

For transfers outside the EU/EEA and UK, we implement:

- Standard Contractual Clauses (SCCs) with Transfer Impact Assessments and supplemental measures per Schrems II guidance
- Adequacy decisions adopted by the European Commission or the UK authorities

- Binding Corporate Rules, where applicable

Privacy Contact (and EU/EEA Representative):

Jonathan Elinsky

LearnQuest Incorporated

1900 Market Street, Suite 800

Philadelphia, PA 19103, USA

Tel: +1 (610) 206-0101

LearnQuest appoints a Privacy Contact rather than a mandatory DPO, as our core activities do not involve large-scale sensitive data processing or systematic monitoring requiring a GDPR-mandated DPO.

6. Data Retention

We retain personal data only as long as necessary to fulfill the purposes described and to comply with legal obligations. We maintain documented operational procedures for retention and secure deletion of data, which are reviewed by our audit and compliance teams to ensure adherence to these timeframes.

Data Category	Retention Period	Legal Justification
Payment & transaction records	7 years	Tax/legal obligations
Certification/educational records	10 years	Accreditation & compliance
Account data (inactive)	5 years of inactivity	Legitimate interest / business need
Marketing data	Deleted 24 months after the later of the last marketing email engagement (e.g., link click) or most recent consent renewal	Consent
Support inquiries	24 months	Legitimate interests
Analytics & advertising event data	GA4 default (14 months); aggregated de-identified metrics retained longer where permissible	Platform settings & de-identified use

7. Your Rights and Choices

7.1 EU/EEA & UK GDPR Rights

You may:

- Access, correct, or delete your personal data
- Restrict or object to processing
- Receive your data in a portable format
- Withdraw consent at any time
- Lodge a complaint with a supervisory authority

7.2 U.S. State Privacy Rights

Residents of California, Virginia, Colorado, Connecticut, Utah, and other U.S. states with applicable consumer data protection laws have rights similar to those outlined under the GDPR and CCPA/CPRA.

These rights may include:

- Requesting disclosure of personal data categories and specific pieces collected, shared, or sold in the past 12 months
- Requesting deletion or correction of personal data
- Opting out of targeted advertising and sale/sharing of personal data
- Limiting use of sensitive personal information (e.g., financial account, precise geolocation, racial or ethnic origin)
- Designating an authorized agent to exercise these rights

Requests may be submitted via Privacy.Compliance@learnquest.com, and we will verify your identity before processing.

If you would like LearnQuest to remove your personal information from our systems, please [fill out this form](#) and send it to our Privacy Compliance Team.

Ongoing Compliance: LearnQuest actively monitors new and emerging state privacy laws (currently more than 19 across the U.S.) and updates our practices and disclosures as additional regulations take effect. We extend comparable rights and protections to residents of any state with an active consumer data protection law, ensuring consistency and compliance nationwide.

7.3 Opt-Out Mechanisms

- Use the “Do Not Sell or Share My Personal Information” link in the site footer
- Send an opt-out request to Privacy.Compliance@learnquest.com
- Global Privacy Control (GPC) signals sent from your browser will be honored as valid opt-out requests

8. CCPA/CPRA 12-Month Disclosure Table

Category	Collected	Disclosed to Service Providers	Shared for Targeted Ads
Identifiers	Yes	Yes	Yes
Commercial Information	Yes	Yes	No
Internet/Network Activity	Yes	Yes	Yes
Geolocation Data	Yes	Yes	Yes
Professional Information	Yes	Yes	No
Inferences	Yes	Yes	Yes

9. Children's Privacy

For minors, we implement robust parental consent verification methods, such as credit-card verification, parental email confirmation, or other industry-standard age verification processes. We apply strict data minimization principles, and provide an “eraser button” for easy deletion. These procedures are designed to ensure compliance with COPPA, COPPA 2.0, and applicable child data protection standards globally. If you believe we have collected data from a minor, contact Privacy.Compliance@learnquest.com for prompt deletion.

10. Automated Decision-Making & Profiling

We do not currently engage in automated decision-making that produces legal or similarly significant effects. Should we implement algorithmic training recommendations, learner risk scoring, or similar profiling features in the future, we will update this Policy, explain the logic involved, and provide a clear opt-out mechanism.

11. Data Minimization & Accuracy

We collect only the minimum personal data necessary for specified purposes. We take reasonable steps to ensure data accuracy and update it upon request. We conduct quarterly data minimization reviews and automatically remove or anonymize data that is no longer required for our stated purposes. These reviews

and automated controls ensure compliance with GDPR Article 5(1)(c) and other global minimization standards. Our documented procedures also define the specific workflows, responsibilities, and audit logs for data deletion and anonymization, ensuring full accountability and regulatory traceability.

12. Data Security

We maintain administrative, technical, and organizational measures—encryption at rest and in transit, access controls, role-based permissions, secure development practices, and regular audits/penetration testing—to protect personal data. We continuously review and enhance our security posture.

13. Data Breach Notification

In the event of a data breach affecting personal data:

- We will notify the relevant supervisory authority within 72 hours if required under GDPR.
- We will inform affected individuals without undue delay if there is a high risk to their rights and freedoms.
- Notifications will include the nature of the breach, categories of data involved, likely consequences, and measures taken to mitigate harm.

14. Email Marketing (CAN-SPAM Compliance)

All commercial emails comply with the CAN-SPAM Act and include:

- Accurate sender identification and subject lines
- Our valid physical mailing address
- Clear unsubscribe instructions; opt-out requests processed within 10 business days

Transactional and service-related emails are not subject to unsubscribe requests.

15. Changes to This Policy

We may update this Policy periodically. Material changes will be communicated via email or a prominent notice on our website. Continued use of our services after updates indicates acceptance of the revised Policy.

16. Contact Us

For questions or to exercise your rights:

- General inquiries: info@learnquest.com
- Privacy & compliance: Privacy.Compliance@learnquest.com

Privacy Contact & EU/EEA Representative:

LearnQuest Incorporated
1900 Market Street, Suite 800
Philadelphia, PA 19103, USA
Tel: +1 (610) 206-0101