Privacy Policy

Last Updated: October 3, 2026

The Pre-Law Network respects the privacy of its members.

This Privacy Policy explains how **Dean Beardsworth**, as the host of **The Pre-Law Network** website ("The Pre-Law Network," "we," "us," or "our"), collects, uses, discloses, retains, and protects personal information through **theprelawnetwork.com** and related services.

We intend to manage personal information in accordance with applicable Canadian privacy law, including the **Personal Information Protection and Electronic Documents Act ("PIPEDA")** where applicable.

1. Scope

This Privacy Policy applies to personal information collected through:

- The Pre-Law Network website;
- account registration;
- student, professional, and society applications;
- verification procedures;
- member profiles;
- directories;
- posts and other user content;
- member interactions and communications;
- support communications;
- events or programs operated through the Network; and
- paid services where offered.

2. Personal Information We Collect

The information we collect depends on how you use the Network.

Account Information

We may collect:

- name;
- email address;
- account credentials;
- account type;
- institutional or organizational affiliation;
- graduation year or year of study;

- location information you choose to provide; and
- other information needed to establish or administer an account.

Student Information

For Student Accounts, we may collect information such as:

- university or post-secondary institution;
- undergraduate program;
- year of study;
- participating pre-law society or student organization;
- expected graduation year;
- legal interests;
- professional interests;
- achievements;
- hobbies;
- work experience;
- biography; and
- other profile information voluntarily provided by the student.

Proof of Enrolment

We may request reasonable documentation or information to verify that an applicant is currently enrolled in an eligible undergraduate program.

Verification documentation is collected for the purpose of determining eligibility and preventing fraudulent accounts.

Where reasonably possible, we will retain only the information necessary to record that verification occurred rather than retaining complete verification documents indefinitely.

Professional Information

Professional applicants may provide information such as:

- name;
- professional title;
- employer or organization;
- location;
- professional biography;
- education;
- areas of law or professional interest;
- work experience;
- professional contact information;
- licensing or professional-status information; and
- information reasonably necessary to review an application.

Society and Organization Information

We may collect:

- organization name;
- institution;
- membership size;
- names and contact information of authorized representatives;
- society logos;
- organization descriptions;
- membership information necessary to administer participation;
- account administrator information; and
- other information submitted through the society application process.

Profile and User Content

We collect information that users voluntarily add to the Network, including:

- profile photographs;
- biographies;
- achievements;
- experience;
- interests;
- posts;
- photographs or other uploaded media;
- opportunity listings;
- society information; and
- other content submitted through the Network.

Network Activity

We may collect information about how users interact with the Network, such as:

- connections;
- profile interactions;
- posts and engagement;
- account activity;
- reports;
- invitations;
- application status; and
- use of particular Network features.

Communications

Where the Network provides messaging or other communication functionality, communications transmitted through the platform may be stored as necessary to provide that functionality.

We do not treat private communications as public profile information.

Authorized personnel may access communications where reasonably necessary to:

- investigate a safety or abuse report;
- respond to a user support request;
- prevent fraud or misuse;
- maintain platform security;
- comply with law; or
- enforce our Terms of Use.

We do not access private communications simply out of curiosity or for unrelated purposes.

Payment Information

If paid services are offered, we or our payment service providers may collect information necessary to process payments.

Payment card details may be processed directly by a third-party payment processor rather than stored by The Pre-Law Network.

We may retain transaction information such as:

- amount paid;
- subscription type;
- transaction date;
- billing status; and
- information required for accounting, taxation, dispute resolution, or legal compliance.

Technical Information

When users access the Network, we may automatically receive information such as:

- IP address;
- browser type;
- device type;
- operating system;
- login activity;
- pages or features accessed;
- approximate geographic information derived from technical data;
- referring pages; and
- diagnostic or security information.

3. How We Collect Information

We may collect personal information:

- directly from you;
- through your participating society or organization where appropriate;
- when another authorized user invites you;
- through applications and verification procedures;

- through your use of Network features;
- automatically through website technology;
- from publicly available professional sources where appropriate; or
- from service providers assisting us in operating the Network.

Where information is obtained from another source, we will use it only where permitted by applicable law.

4. Why We Use Personal Information

We use personal information for purposes including:

Providing the Network

To:

- establish accounts;
- authenticate users;
- provide profiles and directories;
- enable networking and connections;
- provide society pages;
- operate posts and community features;
- administer applications; and
- provide requested services.

Verification

To:

- verify student eligibility;
- verify society affiliation;
- assess professional applications;
- prevent impersonation;
- detect fraudulent accounts; and
- protect the integrity of the Network.

Member Discovery

Certain profile information is used to allow approved members to discover relevant students, professionals, societies, organizations, and opportunities.

Safety and Security

We may process personal information to:

- secure accounts;
- investigate suspected misuse;
- respond to reports;
- detect fraud;

- prevent unauthorized access;
- enforce our Terms of Use; and
- protect members and the Network.

Improving the Network

We may use information about Network activity to understand how features are used, diagnose problems, improve functionality, and develop the Network.

Where reasonably possible, aggregated or de-identified information will be used for analysis rather than personally identifiable information.

Communications

We may use contact information to send:

- account verification messages;
- security notices;
- application updates;
- service announcements;
- administrative communications;
- requested information; and
- promotional communications where legally permitted.

Billing and Administration

Where paid services are offered, we may process information to administer subscriptions, invoices, payments, taxes, cancellations, and disputes.

Legal Compliance

We may use or disclose information where reasonably necessary to comply with applicable law, court orders, lawful governmental requests, professional obligations, or legal proceedings.

5. Profile Visibility

The Network is designed to facilitate professional connections.

Information intentionally placed in a member profile may therefore be visible to other authorized members of the Network.

The exact visibility of information may depend on:

- account type;
- privacy settings;
- Network features;
- membership status; and
- the context in which the information was submitted.

Users should not place information in member-visible portions of their profile that they do not want other authorized members to see.

Verification documentation, payment information, passwords, administrative records, and other information identified as non-public are not treated as public profile information.

6. Sharing Personal Information

We do not sell or rent member personal information or member contact lists.

We may disclose personal information in the following circumstances.

Other Network Members

Profile information and content intended for member visibility may be displayed to other authorized Network users.

Participating Societies and Organizations

Where necessary to administer membership or organizational participation, limited information may be shared with an authorized society or organization representative.

We will not provide societies unrestricted access to information that is unrelated to administering their participation.

Service Providers

We may use third-party service providers for services such as:

- website hosting;
- cloud infrastructure;
- authentication;
- email delivery;
- data storage;
- analytics;
- security;
- payment processing; and
- technical support.

Service providers receive access only to information reasonably necessary to provide their services and are expected to handle information in accordance with applicable contractual and legal obligations.

Business Transactions

If The Pre-Law Network undergoes a merger, acquisition, financing, restructuring, or sale of all or part of the business, personal information may be disclosed as permitted by applicable law and subject to appropriate protections.

Legal and Safety Requirements

We may disclose personal information where required or permitted by law or where reasonably necessary to protect the rights, safety, or security of The Pre-Law Network, our members, or others.

7. Consent

Where consent is required, we seek consent that is appropriate to the nature and sensitivity of the information and the reasonable expectations of the individual.

We will identify the purposes for collecting personal information at or before the time it is collected.

We will not require users to consent to unnecessary collection, use, or disclosure of personal information as a condition of receiving a service.

Where we propose a materially new use of personal information that requires additional consent, we will seek that consent before using the information for that purpose.

8. Marketing Communications

We may send promotional electronic communications where permitted by law.

Where required, we will obtain appropriate consent.

Commercial electronic messages will contain information identifying the sender and an appropriate method of unsubscribing where required by applicable law.

Users may withdraw consent to promotional communications at any time.

Service, security, verification, billing, and other non-promotional account communications may still be sent where reasonably necessary.

9. Cookies and Similar Technologies

The Network may use cookies or similar technologies to:

- maintain login sessions;
- remember user preferences;
- secure accounts;
- understand website usage;
- diagnose technical problems; and
- improve performance.

Where non-essential tracking technology requires consent, we will provide an appropriate choice.

Information about specific analytics or advertising providers should be disclosed where applicable.

10. Retention

We retain personal information only for as long as reasonably necessary for the purposes for which it was collected or as required for legitimate legal, security, accounting, fraud-prevention, or dispute-resolution purposes.

Retention periods may vary depending on the type of information.

When personal information is no longer reasonably required, we will take reasonable steps to securely delete, destroy, or de-identify it.

Verification Documents

Because enrolment and identity verification documents may contain more information than is necessary for ongoing operation of an account, our goal is to minimize their retention.

Where reasonably possible, after verification we will retain a record indicating that verification was completed rather than indefinitely retaining the complete document.

11. Account Closure and Deletion

Users may request closure of their accounts.

Following account closure, certain information may be deleted, de-identified, or removed from active systems.

Some information may be retained where reasonably necessary for:

- security;
- fraud prevention;
- financial records;
- dispute resolution;
- enforcement;
- backups;
- legal obligations; or
- establishing or defending legal claims.

Content previously shared with other users may not disappear from copies lawfully retained by those users.

12. Accuracy

Users may update much of their account and profile information directly through the Network.

We encourage users to keep important information reasonably accurate and current.

Users may also request correction of personal information held by us where appropriate.

13. Security

We use administrative, technical, and organizational safeguards appropriate to the sensitivity of the personal information in our control.

Measures may include:

- account authentication;
- access controls;
- restricted administrative access;
- secure hosting;
- encryption where appropriate;
- security monitoring;
- software updates;

- backups; and
- internal procedures governing access to personal information.

No online service can guarantee absolute security.

Users should use strong passwords, protect their credentials, and notify us promptly if they suspect unauthorized access.

14. Privacy and Security Incidents

We maintain procedures for responding to suspected privacy and security incidents.

Where applicable law requires notification of a privacy breach, we will notify affected individuals and applicable regulatory authorities as required.

We will maintain records of security breaches where required by law.

15. Processing Outside Your Province or Canada

Some service providers may process or store information in another province, territory, or country.

When personal information is processed in another jurisdiction, it may be subject to the laws of that jurisdiction.

We remain responsible for personal information under our control and will use reasonable contractual and organizational measures when engaging service providers.

16. Access to Your Personal Information

Subject to applicable legal exceptions, individuals may request information about personal information we hold about them.

A request may include asking:

- whether we hold personal information about you;
- how that information has been used;
- to whom it has been disclosed;
- for access to the information; or
- for inaccurate or incomplete information to be corrected.

We may take reasonable steps to verify your identity before responding.

17. Withdrawal of Consent

Where personal information is processed on the basis of consent, users may withdraw consent subject to legal or contractual restrictions and reasonable notice.

Withdrawal may affect our ability to provide services that require the relevant information.

For example, withdrawing consent to the processing of information necessary to maintain a verified member account may require that the account be closed.

18. Children and Younger Users

The Pre-Law Network is designed primarily for post-secondary students and professionals and is not intended for children under 13.

If we learn that personal information has been collected from a child who cannot provide meaningful consent without appropriate parental or guardian authorization, we will take appropriate steps consistent with applicable law.

19. Privacy Complaints

Individuals may contact us with questions or concerns about our handling of personal information.

We will investigate privacy complaints reasonably and in good faith.

Nothing in this Policy limits an individual's right to contact an applicable privacy regulator.

20. Privacy Officer

The Pre-Law Network designates a person responsible for privacy compliance.

Privacy requests, access requests, correction requests, and complaints may be directed to:

Privacy Officer

Dean Beardsworth

The Pre-Law Network

Email: **dbeardsw@uwo.ca**

21. Changes to this Privacy Policy

We may update this Privacy Policy as the Network, technology, or applicable legal requirements change.

The current version will be made available through the Network.

Where changes materially affect how personal information is collected, used, or disclosed, we will provide appropriate notice and obtain additional consent where required.

22. Contact

Questions about this Privacy Policy may be directed to:

The Pre-Law Network

Email: **dbeardsw@uwo.ca**

Website: **theprelawnetwork.com**