# PRIVACY POLICY

**Never Summit Privacy Policy**
**Effective Date:** June 4, 2026
**Version:** 1.0

This Privacy Policy explains how **Never Summit LLC** (hereinafter referred to as the "Company") collects, uses, discloses, stores, and protects personal information through Never-Summit.com, and related services.

This Privacy Policy applies to Students, Mentors, Employers, recruiters, Universities, institutional administrators, visitors, and any other users.

**1. Summary.** The Company operates a student career, mentorship, recruiting, and university engagement platform. Depending on your role and settings, we may collect and process information such as contact information, student profile information, photos, resumes, GPA, major, graduation year, gender, work experience, narrative responses, mentoring requests, employer interactions, LinkedIn profile, relocation preferences, university affiliation, payment information, and communications.

Student information may be shared with authorized Universities, Mentors, Employers, recruiters, and Platform administrators depending on the features used, program participation, account settings, and applicable agreements.

## 2. Information We Collect

**2.1 Account Information.** We may collect:

1. Name.
2. Email address.
3. Phone number.
4. Password or authentication credentials.
5. Account role.
6. Organization name.
7. Title or position.
8. Profile photo.
9. Account settings.
10. Login and security information.

**2.2 Student Profile Information.** Students may provide, or Universities may upload, information such as:

1. Name.
2. Email address.
3. Phone number.
4. University or school affiliation.

5. Student ID or institutional identifier, if provided by an Institution.
6. Major, minor, department, academic program, or field of study.
7. Graduation year or expected graduation date.
8. GPA or academic indicators.
9. Gender, pronouns, or demographic information, if collected.
10. Domestic or international student status, if collected.
11. Citizenship, immigration, visa, sponsorship, CPT, OPT, STEM OPT, or work-authorization information, if collected.
12. Resume, CV, transcript, portfolio, writing sample, or uploaded documents.
13. Photo, video, media, or profile image.
14. LinkedIn profile, portfolio links, GitHub links, personal website, or social/professional links.
15. Work experience, internships, projects, skills, certifications, awards, and activities.
16. Career interests, job preferences, relocation preferences, availability, and desired opportunities.
17. Narrative responses, essays, statements, mentoring goals, personal story fields, and profile text.
18. Mentor requests, accepted mentor relationships, session notes if entered, and related communications.

**2.3 International Student Information.** For International Students, the Platform may collect or allow students to provide information related to:

1. International student status.
2. Visa type or immigration category.
3. CPT, OPT, STEM OPT, or other work-authorization status.
4. Sponsorship needs.
5. Work eligibility.
6. Country of citizenship or residence, if provided.
7. Relocation or geographic preferences.
8. Employment timing or authorization constraints.

We use this information only as described in this Policy and the Platform. Employers and recruiters may use this information only for lawful recruiting and employment-related purposes and may not use it for unlawful discrimination.

The Platform does not provide immigration advice.

**2.4 Mentor Information.** For Mentors, we may collect:

1. Name and contact information.
2. Profile photo.
3. Biography.
4. Credentials, education, employment history, and expertise.
5. Availability.
6. Booking links.

7. Contact details.
8. Session pricing.
9. Payment or payout information.
10. Mentor communications.
11. Ratings, feedback, or program participation data if enabled.

**2.5 Employer and Recruiter Information.** For Employers and recruiters, we may collect:

1. Name.
2. Work email.
3. Phone number.
4. Company name.
5. Job title.
6. Hiring role.
7. Company profile.
8. Job postings or opportunities.
9. Candidate searches.
10. Candidate saves, views, messages, notes, and contact activity.
11. Subscription or billing information.
12. Candidate access acknowledgments.
13. Compliance certifications and acceptance records.

**2.6 University and Institutional Information.** For Universities and institutional users, we may collect:

1. Administrator name.
2. Work email.
3. Phone number.
4. Institution name.
5. Department, program, or career center.
6. Account configuration.
7. Student rosters or CSV imports.
8. Program participation data.
9. Uploaded institution content.
10. Institutional files.
11. Student visibility settings.
12. Employer or mentor access settings.
13. Certification and import acknowledgment records.
14. Data-processing, FERPA, and administrative records.

**2.7 Payment Information.** If you purchase a paid service, subscription, mentor session, employer plan, or institutional service, our payment processor may collect payment card details, billing address, transaction data, and related payment information. We generally do not store full payment-card numbers. Payment processing is handled by a third-party payment processor, Stripe.

**2.8 Communications.** We may collect messages, emails, chat messages, mentor requests, employer communications, support requests, feedback, survey responses, and other communications sent through or about the Platform.

**2.9 Device, Usage, and Technical Information.** We may collect:

1. IP address.
2. Device identifiers.
3. Browser type.
4. Operating system.
5. Referring pages.
6. Pages viewed.
7. Dates and times of access.
8. Clicks, searches, and usage events.
9. Approximate location based on IP address.
10. Log data.
11. Cookies and similar technologies.
12. Security and fraud-prevention signals.

**3. Sources of Information.** We may collect information from:

1. You directly.
2. Universities and Institutions.
3. Employers and recruiters.
4. Mentors.
5. Other users.
6. Payment processors.
7. Authentication providers.
8. Calendar, video, or communication tools.
9. Analytics and hosting providers.
10. Publicly available sources, where permitted.
11. Third-party integrations that you authorize.

**4. How We Use Information.** We use information to:

1. Create and manage accounts.
2. Provide student profiles and career-development tools.
3. Support mentoring and mentor requests.
4. Support employer recruiting and candidate search.
5. Support University programs and student engagement.
6. Display profiles to authorized users.
7. Process resume, media, and file uploads.
8. Facilitate bookings, payments, subscriptions, and session purchases.
9. Send transactional communications.
10. Send marketing communications where permitted.
11. Respond to support requests.

12. Personalize user experience.
13. Improve, test, and develop Platform features.
14. Analyze usage and performance.
15. Secure the Platform.
16. Prevent fraud, scraping, abuse, and unauthorized access.
17. Enforce legal terms and policies.
18. Comply with legal obligations.
19. Protect rights, safety, and security.
20. Create deidentified, aggregated, or statistical information.

**5. Student Data Sharing.** Depending on settings, program participation, and Platform features, Student information may be shared with:

1. The Student's University or Institution.
2. University administrators, career center staff, mentors, and program managers.
3. Mentors who receive or accept mentor requests.
4. Employers and recruiters with authorized candidate-search access.
5. Employers or recruiters who access contact details for recruiting purposes.
6. Platform administrators and support staff.
7. Service providers that help operate the Platform.
8. Payment processors, if paid features are used.
9. Legal, regulatory, or safety-related parties where required or appropriate.

Student profiles, resumes, photos, videos, GPA, gender, narrative responses, contact information, LinkedIn profile, relocation preference, university affiliation, and international-student/work-authorization information may be visible to authorized users if the Platform settings, program configuration, or Student choices permit that visibility.

The Company does not sell Student Data, Institution Student Data, education records, or Candidate Data to third parties for monetary consideration. Any disclosures are made solely for Platform operations, recruiting, mentorship, educational engagement, service delivery, legal compliance, or other purposes described in this Privacy Policy.

**6. Employer Access to Candidate Data.** Employers and recruiters may receive access to Candidate Data for recruiting, hiring, internship, career placement, mentorship, professional opportunity, or related talent-development purposes.

Employers and recruiters may not use Candidate Data for scraping, resale, redisclosure, unrelated advertising, unlawful screening, unlawful discrimination, or unauthorized profiling.

**7. University-Provided Student Data.** Universities may upload or import Student data into the Platform.

The University is responsible for ensuring that it has the legal authority, notices, consents, FERPA basis, contractual basis, institutional authority, and accuracy required to provide Student data to the Platform.

Where applicable, we process Institution Student Data according to the University's instructions, applicable agreements, and permitted Platform purposes.

**8. FERPA-Related Notice.** If a University subject to FERPA provides Student education records or personally identifiable information from education records to the Platform, the University is responsible for determining the applicable FERPA basis.

Depending on the arrangement, the Platform may function as a contractor, consultant, outsourced service provider, or school official for the Institution. In that case, we will use the information only for authorized purposes and will not knowingly redisclose it except as permitted by the University, applicable agreement, or law.

Students should contact their University for FERPA rights related to education records maintained by the University.

**9. Sensitive Information.** The Platform may process information that some laws treat as sensitive, including demographic information, citizenship or immigration information, precise location if enabled, data relating to known minors, or other sensitive information.

We do not knowingly sell sensitive personal data.

We do not use photos for facial-recognition identification unless expressly disclosed and separately authorized.

We do not make final hiring, employment, education-enrollment, or immigration decisions.

The Company operates a technology platform that facilitates connections and interactions among Students, Mentors, Employers, recruiters, Universities, and other users. The Company is not a party to any employment relationship, internship arrangement, mentorship relationship, admissions decision, sponsorship decision, immigration matter, professional engagement, or other relationship formed between users through the Platform.

**10. Domestic and International Students.** We protect Student data regardless of whether a Student is domestic or international.

International Student information may be used to support recruiting, career placement, mentorship, sponsorship-related discussions, and employer understanding of work-authorization timing, where lawful.

Employers remain responsible for complying with employment, immigration, work-authorization, sponsorship, anti-discrimination, and document-verification laws.

**11. Cookies and Similar Technologies.** We may use cookies, pixels, local storage, analytics tools, and similar technologies to:

1. Keep users signed in.

2. Remember preferences.
3. Secure accounts.
4. Measure usage.
5. Improve performance.
6. Understand feature adoption.
7. Support marketing, where permitted.

You may control cookies through your browser settings. Some features may not work properly if cookies are disabled.

**12. Marketing Communications.** We may send marketing emails about Platform features, events, opportunities, updates, or services where permitted by law.

You may opt out of marketing emails by using the unsubscribe link or contacting us at **support@never-summit.com.**

Even if you opt out of marketing emails, we may still send transactional messages, including account notices, security alerts, billing notices, legal notices, and service-related messages.

**13. Service Providers.** We may share information with service providers that help us operate the Platform, including:

1. Cloud hosting providers.
2. Email and communication providers.
3. Payment processors.
4. Analytics providers.
5. Customer support tools.
6. Security and fraud-prevention providers.
7. File storage providers.
8. Calendar and video tools.
9. Resume processing or parsing providers.
10. Professional advisors.

Service providers may access information only as needed to provide services to us and subject to contractual obligations where applicable.

**14. Legal, Safety, and Compliance Disclosures.** We may disclose information if we believe disclosure is reasonably necessary to:

1. Comply with law, legal process, or government request.
2. Enforce our Terms or policies.
3. Protect rights, safety, or security.
4. Investigate fraud, abuse, harassment, or security incidents.
5. Prevent harm to users or the public.
6. Respond to claims or disputes.
7. Support audits, compliance reviews, or institutional obligations.

**15. Business Transfers.** If we are involved in a merger, acquisition, financing, reorganization, sale of assets, bankruptcy, or similar transaction, information may be disclosed or transferred as part of that transaction, subject to applicable law and contractual obligations.

**16. Deidentified and Aggregated Data.** We may create and use deidentified, anonymized, aggregated, or statistical data for analytics, research, product improvement, reporting, benchmarking, and business purposes. We will not attempt to reidentify deidentified data except as permitted by law.

The Platform may use artificial intelligence, machine learning, search, matching, recommendation, automation, analytics, and similar technologies to improve Platform functionality, assist users, facilitate recruiting and mentorship activities, improve user experience, and develop Platform features. To the extent such technologies are used for training or improvement purposes, the Company may use deidentified, aggregated, anonymized, or otherwise non-personally identifiable information. The Company does not use personal information to make final employment, admissions, immigration, or legal decisions.

**17. Data Retention.** We retain information for as long as reasonably necessary for the purposes described in this Privacy Policy, including:

1. While your account is active.
2. As needed to provide the Platform.
3. As required by University or Employer agreements.
4. As needed for legal, tax, accounting, audit, security, or compliance purposes.
5. As needed to resolve disputes.
6. As needed to enforce agreements.
7. As required by applicable law.

Backups and logs may persist for a limited period after deletion.

Institution Student Data may be retained, returned, or deleted according to the applicable institutional agreement and legal requirements.

**18. Security.** We use reasonable administrative, technical, and physical safeguards designed to protect personal information. These safeguards may include access controls, encryption where appropriate, monitoring, authentication, vendor controls, logging, and internal policies. No online service is completely secure. You are responsible for protecting your login credentials and using secure devices and networks.

While the Company implements reasonable safeguards designed to protect personal information, no method of transmission over the Internet, electronic storage system, or security measure is guaranteed to be completely secure. Accordingly, the Company cannot and does not guarantee absolute security and disclaims liability for unauthorized access, disclosure, loss, alteration, or destruction of information except to the extent required by applicable law.

**19. Data Breach Notice.** If we determine that a security incident requires notice under applicable law, we will provide required notices to affected individuals, institutions, regulators, or other parties in accordance with applicable law.

**20. Your Privacy Choices.** Depending on your role, account settings, location, and applicable law, you may be able to:

1. Access certain personal information.
2. Correct certain personal information.
3. Delete certain personal information.
4. Export certain personal information.
5. Restrict or object to certain processing.
6. Opt-out of marketing emails.
7. Adjust profile visibility settings.
8. Disable certain optional fields.
9. Request information about sharing.
10. Appeal certain privacy-rights decisions where required by law.

Requests may be submitted to **support@never-summit.com**

We may need to verify your identity before fulfilling a request.

**21. Florida Privacy Rights.** If Florida privacy law applies to the Company or to a specific processing activity, Florida residents may have rights to access, correct, delete, obtain a copy of personal data, opt out of certain targeted advertising, opt out of the sale of personal data, opt out of certain profiling, opt out of certain sensitive-data processing, and appeal certain decisions.

Even where a specific Florida privacy statute does not apply to us because of threshold requirements or exemptions, we may choose to honor reasonable privacy requests as a matter of policy, subject to legal, contractual, technical, security, and operational limitations.

**22. Other U.S. State Privacy Rights.** Residents of certain U.S. states may have additional privacy rights. We will respond to verified requests as required by applicable law.

**23. International Users and Data Transfers.** The Company is based in the United States. If you access the Platform from outside the United States, your information may be transferred to, stored in, accessed from, or processed in the United States and other countries that may not provide the same level of data protection as your country.

Where required, we rely on appropriate legal mechanisms for international transfers, such as consent, contractual necessity, legitimate interests, standard contractual clauses, data-processing agreements, or other lawful transfer mechanisms.

**24. EEA, UK, and Swiss Users.** If applicable law gives you rights under the GDPR, UK GDPR, or similar laws, you may have rights to:

1. Access your personal data.
2. Correct inaccurate personal data.
3. Delete personal data.
4. Restrict processing.
5. Object to processing.
6. Receive a portable copy of personal data.
7. Withdraw consent where processing is based on consent.
8. Lodge a complaint with a supervisory authority.

The legal bases for processing may include contract performance, legitimate interests, consent, compliance with legal obligations, and protection of rights and safety.

**25. Children and Minors.** The Platform is not intended for children under 13.

We do not knowingly collect personal information from children under 13 unless specifically authorized through an institutional program, parental consent, or another lawful basis approved by counsel. If you believe a child under 13 has provided personal information without authorization, contact us immediately at **support@never-summit.com.**

If the Platform is used by minors under 18, additional parental, institutional, contractual, or legal requirements may apply.

**26. Profile Visibility Controls.** Depending on your role and settings, you may be able to control whether certain profile fields are visible to Universities, Mentors, Employers, recruiters, or other authorized users. Some information may remain visible to your University, Platform administrators, or other authorized parties if required for account administration, program participation, security, legal compliance, or contractual obligations.

**27. User Responsibility for Shared Information.** Users are responsible for the accuracy of information they provide and for determining what information they choose to include in profiles, resumes, messages, mentor communications, applications, and other Platform content. Users acknowledge that information designated as visible to authorized users may be viewed, downloaded, copied, retained, or acted upon by those authorized users in accordance with applicable agreements and Platform functionality.

**28. Automated Processing.** The Platform may use search, filtering, ranking, matching, recommendations, or analytics to help Students, Mentors, Universities, and Employers use the Platform. We do not make final hiring, employment, university admission, immigration, or legal decisions on behalf of Employers, Universities, or government agencies. Employers and Universities are responsible for their own decisions and legal compliance.

**29. Changes to This Privacy Policy.** We may update this Privacy Policy from time to time. If we make material changes, we will provide notice through the Platform, by email, or by other reasonable means. The updated Privacy Policy will be effective as of the date stated in the updated version.

**30. Third-Party Conduct.** The Company is not responsible for the conduct, actions, decisions, communications, hiring decisions, admissions decisions, mentorship advice, representations, omissions, policies, security practices, or legal compliance of any Student, Mentor, Employer, recruiter, University, Institution, or other third party using the Platform. Users interact with third parties at their own discretion and risk.

**31. Contact.** Privacy questions or requests may be sent to:

**Never Summit LLC**
**Email:** support@never-summit.com
**Website:** never-summit.com