PRIVACY POLICY
NexTrack Consulting Private Limited

Effective Date: 12th March 2026
Last Updated: 12th March 2026

This Privacy Policy applies to all users of www.nextrackconsulting.com — individual clients (students, parents, guardians), corporate entities and their HR teams, and Eligible Employees and Beneficiaries accessing the Employee Benefit Programme. It is fully updated for the Digital Personal Data Protection Rules, 2025.

1. Who We Are

NexTrack Consulting Private Limited ("**NexTrack**," "**we**," "**us**," or "**our**") is the Data Fiduciary for all personal data collected through this Website and in connection with delivering our Services.

Registered Name: NexTrack Consulting Private Limited
GSTIN: 06AAICN7348D1ZE
PAN: AAICN7348D
Delhi NCR Office: WeWork, HQ 27, 6th Floor, Sushant Lok Phase I, Sector 27, Gurugram, Haryana – 122009, India
Mumbai Office: WeWork, Express Towers, Marine Drive, Nariman Point, Mumbai, Maharashtra – 400021, India
Website: www.nextrackconsulting.com

2. Scope of This Policy

This Privacy Policy applies to the following categories of users:

Who	Data Collected by NexTrack
Individual Clients — students, parents, and guardians engaging NexTrack for personal educational consulting	Contact details, academic records, psychometric results, athletic data, essay drafts, communication records
Corporate Clients — companies and entities engaging the Employee Benefit Programme	Entity details, Authorised Signatory information, HR contact details, Eligible Employee enrolment lists (names and email addresses only)
Eligible Employees and Beneficiaries	Same categories as Individual Clients — collected directly from each individual with their own consent
Website Visitors	Usage data, cookies, IP address, inquiry form submissions

This Policy does not apply to third-party websites linked from our Website.

3. Personal Data We Collect

3.1. Individual Clients and Beneficiaries

Category	Examples	Purpose
Identity Data	Full name, date of birth, nationality, photograph	Client identification and onboarding
Contact Data	Email address, phone number, home address	Communication and service delivery
Academic Data	School transcripts, grade reports, test scores (SAT, ACT, TOEFL, AP, IB), subject selections, academic awards	College list development and application guidance
Athletic Data	Sport, position, performance statistics, highlight video links, club/academy affiliations, athletic awards	Student-athlete profiling and coach communication
Psychometric Data	Personality assessment results, career aptitude scores, learning style profiles	Academic and career counseling (Sensitive — explicit consent required)
Financial Data	Fee payment records, instalment history, GST invoice details	Billing, invoicing, GST compliance
Communication Records	Emails, WhatsApp messages, Zoom call summaries, session notes, essay drafts and versions	Service delivery, programme continuity, quality assurance
Application Data	College application details, essays, Common App/UCAS/Coalition App data, offer letters	Application support and outcome tracking

3.2. Corporate Clients

Category	Examples	Purpose
Entity Data	Company name, GSTIN, PAN, registered address, company type	Corporate onboarding, invoicing, GST compliance
Signatory Data	Name, designation, email, phone, IP address and timestamp of digital acceptance	Agreement execution record, contract management

HR Contact Data	Name, email, and designation of HR/Benefits programme administrator	Programme management and account communication
Eligible Employee Data	Employee names and email addresses (only as needed for enrolment into the Programme)	Enrolment into the Employee Benefit Programme. No other employee HR or performance data is collected.

3.3. Website Visitors

i. Usage data: pages visited, time spent, referral source, browser type, device type, operating system;
ii. Technical data: IP address, cookie identifiers, session data;
iii. Inquiry data: name, email, and message submitted through contact or inquiry forms.

4. How We Use Your Data

4.1. All Users

i. Responding to inquiries and providing information about our Services;
ii. Operating and improving our Website;
iii. Complying with legal and regulatory obligations;
iv. Enforcing our Terms of Use and engagement agreements.

4.2. Individual Clients and Beneficiaries

i. Delivering educational consulting services — academic guidance, college list development, application support, essay mentoring, student-athlete profiling, and psychometric counseling;
ii. Communicating via email, WhatsApp, and Zoom;
iii. Maintaining session notes and programme records for continuity of service;
iv. Invoicing, fee collection, and GST compliance;
v. Conducting psychometric assessments (with explicit consent);
vi. With consent: using anonymised testimonials or admission outcomes in marketing materials.

4.3. Corporate Clients

i. Executing and managing the Management Consultancy Agreement;
ii. Onboarding Eligible Employees into the Employee Benefit Programme;
iii. Providing anonymised and aggregated programme utilisation reports to HR/Benefits teams;
iv. Corporate invoicing and GST compliance;
v. Conducting annual programme review meetings.

Employee Privacy Boundary: NexTrack will never share individual Eligible Employee or Beneficiary data — including counselling content, academic strategy, essay drafts, or psychometric results — with the Corporate Client employer. All reporting to employers is anonymised and aggregated only.

5. Legal Basis for Processing

Processing Activity	Legal Basis — DPDPA / Indian Law	Legal Basis — GDPR (EU/EEA Users)
Delivering educational consulting services	Consent (DPDPA); Performance of contract	Art. 6(1)(b) — Contract performance
Psychometric testing and sensitive personal data	Explicit consent (DPDPA; SPDPI Rules 2011)	Art. 9(2)(a) — Explicit consent
Invoicing, GST, and financial records	Legal obligation (GST Act; IT Act; Income Tax Act)	Art. 6(1)(c) — Legal obligation
Corporate onboarding and agreement records	Consent; legitimate interest (contract management)	Art. 6(1)(b) Contract; Art. 6(1)(f) Legitimate interest
Marketing and testimonials	Express consent (DPDPA)	Art. 6(1)(a) — Consent
Website analytics and cookies	Consent (where required); legitimate interest	Art. 6(1)(a) Consent; ePrivacy Directive
Legal compliance and dispute resolution	Legal obligation; legitimate interest	Art. 6(1)(c) Legal obligation; Art. 6(1)(f) Legitimate interest

6. Consent and Notice

In accordance with Rule 3 of the Digital Personal Data Protection Rules, 2025, NexTrack provides a clear notice to Data Principals at or before the point of data collection. This notice identifies: the personal data being collected and its specific purpose; the manner in which consent is given and may be withdrawn; and contact details for the Data Processing Contact and Grievance Officer.

For Individual Clients, consent is obtained through digital acceptance of the Client Engagement Agreement on the NexTrack portal, which incorporates a Schedule of Acknowledgements covering data consent.

For Corporate Clients, consent to process Eligible Employee data for enrolment is obtained through digital acceptance of the Management Consultancy Agreement, under which the Corporate Client also represents it has the requisite authority under applicable employment law to share such data.

For Eligible Employees and Beneficiaries, NexTrack obtains consent directly from each individual through a separate digital acknowledgement on the Client Portal before Services commence.

Note: You may withdraw your consent at any time by contacting us at abhinav@nextrackconsulting.com. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal, and does not entitle you to a refund of fees paid under any engagement agreement.

7. Children and Minors

Many of the students we work with are minors (under 18 years of age). NexTrack takes the protection of children's personal data very seriously and complies with Rule 9 of the DPDP Rules, 2025.

7.1. Parental and Guardian Consent

For any student Beneficiary who is a minor, NexTrack requires verifiable consent from a parent or legal guardian before processing the minor's personal data. This consent is obtained through:

i. The digital acceptance of the Client Engagement Agreement by the parent or guardian (for individual clients); or
ii. A separate digital consent acknowledgement from the parent or guardian of the minor Beneficiary (for the Employee Benefit Programme).

Where required, parental identity may be verified through DigiLocker or equivalent government-issued identity verification.

7.2. No Direct Collection from Minors

NexTrack does not knowingly collect personal data directly from minors without prior parental or guardian consent. If we become aware that personal data of a minor has been collected without proper parental consent, we will delete it promptly.

7.3. Sensitive Data of Minors

Psychometric testing results and academic performance data of minors are treated as sensitive personal data requiring explicit parental consent. Such data is never shared with the Corporate Client employer or any third party without express consent.

8. Corporate Data and the Employee Privacy Boundary

NexTrack maintains a strict Employee Privacy Boundary. The Corporate Client employer will never receive individual-level data about any Eligible Employee's or Beneficiary's counselling sessions, essay content, academic decisions, college choices, or psychometric results.

The following principles govern data processing in the corporate context:

i. Dual Data Fiduciary structure: NexTrack is the Data Fiduciary for individual Eligible Employee and Beneficiary data. The Corporate Client is an independent Data Fiduciary for its own HR and employment data. The Corporate Client does not act as NexTrack's data processor.
ii. Minimum data from employer: NexTrack only accepts from the Corporate Client the information strictly necessary for enrolment — employee names and email addresses. NexTrack does not request or accept employees' HR records, performance reviews, salary information, or any other employment data.
iii. Individual consent: Consent for educational consulting services is obtained directly from each Eligible Employee and Beneficiary. The Corporate Client's acceptance of the Management Consultancy Agreement does not substitute for individual consent.
iv. Aggregated reporting only: All programme utilisation reports provided to the Corporate Client are anonymised and aggregated. No individual-level outcomes, academic data, or personal details are included.
v. Employee exit: When an Eligible Employee leaves the Corporate Client's employment, NexTrack is notified and suspends services. Existing personal data of the employee and their Beneficiaries is handled in accordance with the retention policy in Section 11.

9. Data Sharing and Disclosure

NexTrack does not sell, rent, or trade your personal data to any third party. We share personal data only in the following circumstances:

9.1. Service Delivery

i. NexTrack team members and mentors who need access to your data to deliver the Services;
ii. Communication platforms (WhatsApp, Zoom, Google Meet, email, etc.) used in the course of service delivery — subject to those platforms' own terms and privacy policies;
iii. Google Workspace (Gmail, Drive, Forms) used for document sharing and client intake — subject to Google's privacy policy.

9.2. Institutional Communication

Where explicitly authorised by the client or parent/guardian, NexTrack may communicate a student's profile information to college coaches, admissions offices, or athletic departments as part of the Services. This is done only with clear prior direction from the client and limited to what is necessary.

9.3. Legal Obligations

We may disclose personal data if required to do so by Indian law, court order, regulatory authority, or government body — including to comply with the DPDPA, the IT Act, GST authorities, or tax authorities. We will provide prompt prior notice to the affected user to the extent permitted by law.

9.4. Business Transfers

In the event of a merger, acquisition, or sale of assets, personal data may be transferred to the acquiring entity, subject to the same or equivalent data protection commitments as described in this Policy. Affected users will be notified in advance.

9.5. No Sale of Data

NexTrack does not sell, share for commercial consideration, or otherwise monetise personal data of any user — individual, corporate, or Eligible Employee/Beneficiary.

10. Data Security

In accordance with Rule 8 of the DPDP Rules, 2025 and the SPDPI Rules, 2011, NexTrack implements the following security safeguards:

i. **Encryption:** personal data (including academic and psychometric data) is encrypted in transit (TLS 1.2+) and at rest;
ii. **Access control:** role-based access controls ensure that only authorised NexTrack personnel can access specific categories of personal data;
iii. **Masking and tokenisation:** sensitive data is masked or tokenised where technically feasible in non-production environments;
iv. **Continuous monitoring:** system logs and access records are maintained continuously to detect unauthorised access;
v. **Log retention:** security logs are retained for a minimum of one year in accordance with Rule 8, DPDP Rules 2025;
vi. **Processor contracts:** any third-party service providers who process personal data on our behalf are required to implement equivalent security standards through formal data processing agreements.

While we implement commercially reasonable security measures, no method of transmission over the internet or electronic storage is 100% secure. We encourage users to protect their login credentials and to notify us immediately of any suspected unauthorised access at abhinav@nextrackconsulting.com.

11. Data Retention

We retain personal data only for as long as necessary for the purposes described in this Policy, or as required by applicable law:

Data Category	Retention Period	Basis
Active client data (academic, athletic, communication records)	Duration of Engagement + 12 months minimum	Rule 7, DPDP Rules 2025 — minimum 1-year floor after engagement closes
Psychometric data	Duration of Engagement + 12 months (or as separately consented)	Sensitive data — minimum 1-year floor applies

Financial records (invoices, payment history, GST documents)	8 years from end of relevant financial year	Income Tax Act, 1961; GST Act, 2017
Digital acceptance records (agreements)	Duration of engagement + 7 years	Limitation Act, 1963; IT Act, 2000
Corporate Client entity and signatory data	Duration of engagement + 7 years	Contract records and statutory compliance
Security logs	Minimum 12 months from creation	Rule 8, DPDP Rules 2025
Eligible Employee enrolment data (Corporate)	Duration of engagement + 12 months after employee exits the programme	Rule 7, DPDP Rules 2025
Website visitor and analytics data	12 months from collection	Proportionality and minimal retention

Where you request erasure of your personal data, NexTrack will action this within 48 hours of the pre-erasure notice in accordance with Rule 7 of the DPDP Rules, 2025, subject to legal retention obligations. Security logs remain retained for the mandatory minimum period even after data erasure.

12. Your Rights as a Data Principal

As a Data Principal under the DPDPA, 2023, and as a data subject under the GDPR (for EU/EEA users), you have the following rights in respect of your personal data held by NexTrack:

i. **Right to Access:** Request a summary of the personal data NexTrack holds about you and how it is being processed.
ii. **Right to Correction:** Request correction of inaccurate, incomplete, or outdated personal data.
iii. **Right to Erasure:** Request deletion of your personal data where it is no longer necessary for the original purpose, subject to legal retention obligations.
iv. **Right to Withdraw Consent:** Withdraw consent to processing at any time. Withdrawal does not affect prior lawful processing.
v. **Right to Nominate (DPDPA):** Nominate another individual to exercise your data rights in the event of your death or incapacity.
vi. **Right to Grievance Redressal (DPDPA):** Lodge a grievance with NexTrack's Grievance Officer; if unresolved, escalate to the Data Protection Board of India.
vii. **Right to Data Portability (GDPR):** EU/EEA users may request personal data in a structured, machine-readable format where technically feasible.
viii. **Right to Restrict Processing (GDPR):** EU/EEA users may request restriction of processing in certain circumstances, such as pending a correction request.

To exercise any of these rights, please contact our Data Processing Contact at abhinav@nextrackconsulting.com. Requests will be acknowledged within 72 hours and actioned within 30 days.

Note for Corporate Clients: These rights belong to individual Eligible Employees and Beneficiaries personally, not to the Corporate Client employer. The employer may not exercise data rights on behalf of employees without their express written authorisation.

EU/EEA users who consider that our processing of personal data infringes the GDPR have the right to lodge a complaint with the supervisory authority in their Member State.

13. Cookies and Tracking Technologies

Our Website uses cookies and similar technologies to improve your browsing experience and to understand how the Website is used:

Cookie Type	Purpose	Consent Required?
Strictly Necessary	Essential for the Website to function (e.g., session management, security)	No — essential operation
Analytics / Performance	Understand how visitors use the Website (e.g., Google Analytics)	Yes — consent required
Functional	Remember your preferences and improve user experience	Yes — consent required
Marketing / Tracking	Track visits from marketing channels; measure campaign effectiveness	Yes — consent required

You may manage cookie preferences through your browser settings or through our cookie consent banner when first visiting the Website. For EU/EEA users, our cookie practices comply with the ePrivacy Directive and applicable national implementing laws.

14. Third-Party Links and Platforms

Our Website and Services involve use of the following third-party platforms, each with its own privacy policy:

i. WhatsApp (Meta) — used for client communication;
ii. Zoom — used for video counselling sessions;
iii. Google Workspace (Gmail, Drive, Forms) — used for document sharing and client intake;
iv. Common App, UCAS, Coalition App — college application portals (data entered directly by the student);
v. Social media platforms (Instagram, LinkedIn, YouTube) — linked from the Website for informational purposes.

NexTrack is not responsible for the privacy practices of these platforms. We encourage you to review their individual privacy policies before sharing personal data through them.

15. International Data Transfers

NexTrack is incorporated and operates in India. Personal data is primarily stored and processed in India.

For clients applying to colleges in the United States, United Kingdom, Europe, or other jurisdictions, limited personal data (such as the student's academic profile and athletic résumé) may be shared with institutions and coaches in those countries as part of the Services. Such transfers are made only with the client's or guardian's express direction and consent.

For EU/EEA users, where personal data is transferred outside the EEA, NexTrack ensures appropriate safeguards are in place in accordance with GDPR Chapter V, including reliance on India's DPDPA framework, standard contractual clauses, or other lawful transfer mechanisms as applicable.

The Central Government has not yet notified specific data localisation categories under the DPDPA Rules, 2025. NexTrack will update its practices and this Policy when such notifications are issued.

16. Data Breach Notification Procedure

In accordance with Rule 6 of the DPDP Rules, 2025, NexTrack has a two-tier breach notification protocol:

16.1. Tier 1 — Notification to Affected Individuals

Upon becoming aware of a personal data breach that is likely to affect any Data Principal, NexTrack will notify the affected individual(s) without undue delay. The notice will include:

i. Nature of the personal data that has been breached;
ii. Time and circumstances of the breach (to the extent known);
iii. Likely consequences of the breach on the Data Principal;
iv. Steps NexTrack has taken or proposes to take to address the breach;
v. Contact details of the person to whom the Data Principal may reach out for further information.

16.2. Tier 2 — Report to the Data Protection Board of India

NexTrack will file a detailed breach report with the Data Protection Board of India within 72 hours of becoming aware of a qualifying breach, in the form and manner prescribed under Rule 6 of the DPDP Rules, 2025.

16.3. Corporate Client Notification

Where a breach involves personal data of Eligible Employees or Beneficiaries enrolled under a Management Consultancy Agreement, NexTrack will notify the Corporate Client's designated HR/Benefits contact without undue delay, in addition to notifying the affected individuals

directly. Individual-level breach details will not be shared with the employer unless required to assist in remediation.

If you suspect that your personal data held by NexTrack has been compromised, please contact us immediately at abhinav@nextrackconsulting.com.

17. DPDPA 2023 and DPDP Rules 2025 — Compliance Timeline

The Digital Personal Data Protection Rules, 2025 were notified on 14 November 2025. NexTrack is actively implementing compliance across all phases of the rollout.

Phase	Timeline	Key Requirements	NexTrack Status
Phase I	November 2025 — present	Notice and consent framework (Rule 3); parental/guardian consent for minors (Rule 9); verifiable consent mechanism; breach notification protocol (Rule 6); security obligations (Rule 8)	Implemented — reflected in this Policy and in our Client Engagement Agreement and Management Consultancy Agreement
Phase II	By 13 November 2026	Full enforcement; Data Protection Board operational; penalties up to INR 250 crore; data localisation categories (to be notified); Data Protection Officer appointment (if applicable)	In preparation — compliance roadmap in progress
Phase III	~May 2027 (estimated)	Consent Manager framework; SPDPI Rules 2011 formally superseded; additional sector-specific guidance	To be assessed upon notification

The IT (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (SPDPI Rules) remain in force during the transitional period and continue to apply to the processing of sensitive personal data, including psychometric data and financial information.

18. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, applicable law (including DPDPA Rules notifications), or technology. The "Last Updated" date at the top of this Policy will be revised accordingly.

For material changes — such as changes to the categories of data collected, purposes of processing, or data sharing arrangements — we will notify existing clients and Corporate Clients by email at least 30 days before the changes take effect, and will seek fresh consent where required by the DPDPA or GDPR.

Your continued use of our Website or Services after the effective date of any changes constitutes your acceptance of the updated Policy.

19. Contacts and Grievance Redressal

NexTrack has designated two separate points of contact in accordance with the DPDPA Rules, 2025, reflecting distinct obligations:

19.1. Data Processing Contact — Rule 9 Queries and Data Rights Requests

For questions about how your personal data is processed, to exercise your data rights (access, correction, erasure, withdrawal of consent), or for any privacy-related inquiry:

Name: Mr. Abhinav Nath
Email: abhinav@nextrackconsulting.com
Response time: Acknowledged within 72 hours; actioned within 30 days

19.2. Grievance Officer — Formal Complaints

For formal grievances about NexTrack's data processing practices, in accordance with the IT Act, 2000 and DPDPA, 2023:

Name: Mr. Abhinav Nath
Email: abhinav@nextrackconsulting.com
Address: WeWork, HQ 27, 6th Floor, Sushant Lok Phase I, Sector 27, Gurugram, Haryana – 122009
Response time: Acknowledged within 24 hours; resolved within 15 days

19.3. Escalation — Data Protection Board of India

If your grievance is not resolved to your satisfaction within the timelines stated above, you may escalate your complaint to the Data Protection Board of India once the Board becomes operational (expected by Phase II — November 2026). EU/EEA users may also lodge a complaint with the supervisory authority in their Member State.