Collegeit

CollegeIt

Data Privacy Policy

Version 1.1

Purpose

Flynt Labs Private Limited (herein referred to as “Organization,” “Company,” “we,” “our,” or “us,” etc.) is committed to protecting the privacy of individuals who interact with us. This policy explains how we collect, use, store, and safeguard personal data to ensure transparency and build trust with our users, customers, and partners.The Organization also establishes structured privacy governance, risk assessment, and accountability mechanisms to ensure compliance with applicable data protection laws and regulations.

Scope

This policy applies to all personal data collected through the organization’s websites, applications, services, and other interactions with individuals.This policy also applies to all internal systems, third-party processors, cross-border data transfers, and any new or modified processing activities involving personal data.

Definition

- IP Address: A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.
- Personal Data: Any information relating to an identifiable individual (e.g., name, email, IP address).
- Processing: Any operation performed on personal data, such as collection, storage, use, disclosure, or deletion.
- Data Controller: The entity that determines the purposes and means of processing personal data.
- Data Processor: The entity that processes data on behalf of the data controller.
- Privacy Impact Assessment (PIA/DPIA): A structured process used to evaluate risks to personal data and define mitigation controls before initiating or modifying processing activities.

Responsibilities

- Sanchit Varma, Head of Information Security, privacy@collegeit.org is responsible for developing, implementing, maintaining, and enforcing the policy.
- Employees are responsible and/or accountable to ensure adherence to this policy’s terms during their job duties.
- Data Protection Officer (DPO) / Privacy Officer Responsibilities:
    - Oversee privacy impact assessments (DPIA/PIA)
    - Monitor compliance with data protection laws
    - Maintain records of processing activities and disclosures
    - Handle data subject rights requests and breach notifications

POLICY

Data We Collect

- Applicant contact information: Name, email address and phone number for WhatsApp connections.
- Student ambassador information: Name, email address and phone number supplied by universities for WhatsApp connections and related email reminders.
- Conversation data: WhatsApp message content and voice call transcripts. Voice call recordings are not retained.
- Account information: Username, password and account preferences.

- Technical data: IP address, derived approximate location, device identifiers, operating system, cookies and usage analytics.

We do not request addresses, dates of birth, payment details or sensitive personal data. Users should not include sensitive personal data in messages or voice conversations.

How We Collect Personal Data

- Directly from you: When you fill out forms, create accounts, contact us, send messages or use the voice assistant.
- Automatically: Through cookies, analytics tools and logs when you use our website or services.
- Third parties: From universities, business partners, service providers or publicly available sources.

Legal Bases for Processing Personal Data

We process personal data only when permitted by law. The legal bases include:

- Consent: When you provide explicit consent (e.g., marketing communications).
- Contractual Necessity: To fulfill a contract with you.
- Legal Obligation: To comply with legal and regulatory requirements.
- Legitimate Interests: For fraud prevention, improving services, or ensuring security.

How We Use Personal Data

- Provide and improve our widget, WhatsApp messaging and voice assistance services; facilitate connections and manage accounts.
- Respond to enquiries and support admissions follow-up and student recruitment communications by university admissions and marketing teams.
- Generate conversation insights for university admissions and marketing teams; conduct analytics and research to improve user experience.
- Send student ambassadors email reminders for pending conversation requests; communicate updates and support; ensure security, detect fraud and comply with legal obligations.

Data Sharing and Disclosure

We may share personal data under these circumstances:

- Client universities: Share applicants' names, email addresses and relevant conversation data with their admissions and marketing teams for the purposes described above.
- Service Providers: With vendors or contractors who perform services on our behalf.
- Legal Compliance: To comply with laws, subpoenas, or other legal processes.
- Business Transfers: In the event of mergers, acquisitions, or asset sales.
- Consent: When you explicitly agree to share your data.
- Additional Controls:
    - All disclosures must be logged and recorded, including recipient, purpose, and data shared
    - Third parties must sign data processing agreements (DPAs) with defined privacy obligations
    - Sub-processors must be approved and monitored

Data Retention

We retain personal data only as long as necessary to fulfill the purposes for which it was collected unless a more extended retention period is required by law. Afterward, data is securely deleted or anonymized.

Data Security

We implement industry-standard technical and organizational measures to safeguard personal data, including:

- Encryption (at rest and in transit).
- Access controls and authentication protocols.
- Regular audits and security assessments.
- Personal data shall be securely deleted or destroyed using approved methods such as:
    - Secure wiping / cryptographic erasure
    - Physical destruction of media
- Disposal actions must be logged and verified
- Third-party disposal providers must comply with security requirements

Data Disposal and Destruction

- Personal data shall be securely deleted or destroyed using approved methods such as:
    - Secure wiping / cryptographic erasure
    - Physical destruction of media
- Disposal actions must be logged and verified
- Third-party disposal providers must comply with security requirements

Your Rights

Depending on your jurisdiction, you may have the following rights:

- Access: Request access to your data.
- Rectification: Correct inaccurate or incomplete data.
- Deletion: Request deletion of your data.
- Data Portability: Obtain a copy of your data in a portable format.
- Restriction: Request a limitation on the processing of your data.
- Objection: Object to certain processing activities (e.g., direct marketing).
- Withdraw Consent: Withdraw your consent when processing is based on consent.
- Regular security testing including vulnerability assessments and audits
- Monitoring for unauthorized access and anomalies
- Formal procedures shall exist to handle data subject requests within defined timelines
- All requests must be logged and tracked

To exercise your rights, please contact us at Sanchit Varma, privacy@collegeit.org.

Privacy Impact Assessments (DPIA / PIA)

- Privacy Impact Assessments must be conducted for:
    - New systems or applications
    - New data processing activities
    - Changes to existing processing
- DPIA must evaluate:
    - Risks to individuals
    - Data sensitivity
    - Processing scale
- Mitigation measures must be defined and approved before implementation

Privacy Incident Management & Breach Notification

- All data breaches must be reported immediately to the ISG/DPO
- Incidents must be:
  - Investigated
  - Documented
  - Resolved
- Regulatory and user notifications must be made within legally required timelines
- Root cause analysis and corrective actions must be implemented

Cross-Border Data Transfers

- Personal data transfers outside the originating jurisdiction must comply with applicable laws
- Appropriate safeguards must be implemented, such as:
  - Standard Contractual Clauses (SCCs)
  - Adequacy decisions
  - Binding Corporate Rules (if applicable)

Record Keeping and Accountability

- The Organization shall maintain records of:
  - Processing activities
  - Data disclosures
  - Consent records
  - DPIA assessments
  - Breach incidents
- Records must be retained for audit and compliance purposes

Data Accuracy and Quality Management

- The Organization shall ensure personal data is accurate, complete, and up to date
- Mechanisms shall exist to:
  - Validate data at collection
  - Periodically review and update stored data
- Inaccurate data must be corrected or deleted without delay

Cookies and Tracking Technologies

We use cookies and other tracking technologies to enhance your browsing experience. You can manage your preferences through our cookie policy or browser settings.

Children's Privacy

Our services are intended primarily for prospective postgraduate applicants and are not designed specifically for children. Visitors under 18 may nevertheless use them. Where we become aware that a user is a child, we will assess applicable requirements and take appropriate steps, including obtaining any required authorisation or deleting data where its processing is not permitted. Privacy concerns may be reported to privacy@collegeit.org.

Third-Party Links

Our website or services may contain links to third-party websites. We are not responsible for their privacy practices and encourage you to review their privacy policies.

Updates to This Policy

The organization will update this policy periodically to reflect changes in laws, regulations, or business practices.

Policy updates must be reviewed, approved, and communicated to relevant stakeholders

Version and approval history

Version	Approval date	Status	Approved by	Description
1.0	18 August 2026	Approved	Sanchit Varma	Initial release.
1.1	31 August 2026	Approved	Sanchit Varma	Updated data categories, sources, purposes, university recipients and children’s privacy wording.