Raffles Design International (India) Pvt Ltd
Regd. Office :1st Floor CTS 252 252 1, LBS Marg,
Opp SBI, Kurla West, Mumbai 400070.
+91 98208 22237
www.RafflesMumbai.com
CIN – U74994MH2004PTC147550

DATA PROTECTION & PRIVACY POLICY

Raffles Design International (India) Private Limited

1. Purpose and Objective

This Data Protection & Privacy Policy ("Policy") sets out how the Raffles Design International (India) Private Limited ("RMB" or "the Company") collect, use, store, share and protect digital personal data in accordance with the Digital Personal Data Protection Act, 2023 ("DPDP Act") and applicable rules issued thereunder as notified by the Government of India.

The objectives of this Policy are to:

- Protect the privacy rights of individuals whose personal data we process;
- Ensure lawful, fair, and transparent processing of personal data;
- Define roles, responsibilities and internal controls for DPDP compliance within RMB;
- Provide a framework for handling data breaches, grievances, and data principal rights;

2. Scope and Applicability

This Policy applies exclusively to Raffles Design International (India) Private Limited and governs the processing of all forms of digital personal data handled by RMB, whether collected directly or indirectly, and whether stored digitally or subsequently digitised.

This Policy applies to personal data processed through:

- RMB-owned devices, servers and systems;
- Cloud platforms and collaboration tools such as Microsoft 365, Teams, SharePoint and OneDrive;
- Third-party applications, platforms and service providers engaged by RMB;

This Policy applies to all individuals who access, process or handle personal data on behalf of RMB, including:

- Employees and officers;
- Faculty and visiting faculty;
- Consultants, interns and temporary staff;
- Contractors and service providers.

This Policy covers personal data of, inter alia:

- **Students and applicants** (and their parents/guardians, where applicable)
- **Alumni**
- **Employees and job applicants**

- **Vendors, service providers and partners (including individuals representing organisations)**
- **Visitors to our website(s) and digital platforms**
- **Any other individual whose personal data is processed by RMB.**

3. Key Definitions

- **Digital Personal Data**: Any personal data in digital form about an identifiable individual.
- **Personal Data**: Any data about an individual who is identifiable by, or in relation to, such data.
- **Data Principal**: The individual to whom the personal data relates (e.g. student, parent, employee, vendor contact).
- **Data Fiduciary**: The entity that determines the purpose and means of processing personal data. For the purposes of this Policy, Raffles Design International (India) Private Limited is the Data Fiduciary.
- **Data Processor**: Any third party who processes personal data on behalf of a Data Fiduciary.
- **Processing**: Any operation on personal data, including collection, recording, storage, organisation, use, disclosure, sharing, retrieval, erasure, etc.
- **Significant Data Fiduciary (SDF)**: A Data Fiduciary that may be so notified by the Central Government based on volume/sensitivity of data, risk, etc.
- **Personal Data Breach**: Any unauthorised processing or accidental disclosure, alteration, loss, or destruction of personal data compromising its confidentiality, integrity or availability.

4. Roles and Responsibilities

- **Board of Directors**
  - Approve and oversee this Policy.
  - Allocate adequate resources for data protection and compliance.
- **Data Protection Officer (DPO) / Data Protection Lead**
  - If any entity is notified as a Significant Data Fiduciary, a formal DPO will be appointed.
  - Responsible for the coordination of DPDP compliance; handling queries, grievances, and communication with the Data Protection Board (when required).
- **IT & Security Team**
  - Implement and monitor technical safeguards on systems, networks, and cloud platforms (including Microsoft 365, Teams, etc.).
  - Support breach detection, logging and incident response.

- **HR & Administration**
  - Ensure employee onboarding, employment records and HR systems adhere to this Policy.
  - Incorporate data protection obligations into employment contracts, NDAs, and internal rules.
- **Functional Heads (Academics, Admissions, Legal, Finance, etc.)**
  - Ensure that data processing activities within their functions are compliant (e.g. admissions data, vendor data, finance records, legal files).
- **All Employees and Staff**
  - Must complete any mandated data protection training.
  - Must handle personal data strictly on a "need-to-know" basis and in accordance with this Policy.

5. Lawful Basis for Processing Personal Data

RMB processes personal data only on lawful bases permitted under the DPDP Act, including:

1. **Consent**
   - Obtained from the Data Principal (student, applicant, website user, employee, vendor contact, etc.) before or at the time of collection, where required.
   - Consent will be free, specific, informed, unambiguous and given through clear affirmative action.
2. **Certain Legitimate Uses / Legal Obligations**
   - Where processing is required for performance of legal obligations, employment purposes, compliance with court orders, responding to lawful authorities, or other "certain legitimate uses" as permitted under the DPDP framework (for example, employment-related purposes, prevention of fraud, or enforcing legal claims).

Personal data shall not be processed in a manner incompatible with the purpose for which it was collected, except as permitted by law.

6. Categories of Personal Data and Processing Activities

6.1 RMB (Raffles Design International, Mumbai)

RMB processes personal data in connection with:

- **Admissions & Enrolment**
  - Data collected via admission forms, "Enroll Now" forms, website contact forms, email, phone calls, and in person.
  - Typical data: name, contact details, date of birth, address, education history, portfolio details, identity details (e.g. Aadhaar/passport/pan where required), nationality, parent/guardian details (for minors), academic interests, etc.

- **Academic Administration**
    - Attendance records, internal assessments, exam results, feedback, disciplinary records, learning progress, project submissions, etc.
    - Faculty and staff personal data for timetabling, payroll, performance and administration.
- **Fees, Finance & Scholarships**
    - Billing and payments data, bank details (in limited fields), transaction history, fee-related correspondence, scholarship applications etc.
- **Placements, Internships & Alumni Management**
    - Placement support data, employer information, references, alumni contact information, portfolios, achievements.
- **Marketing, Events & Communications**
    - Use of contact details for information about programmes, events, and newsletters, only as per applicable consent and opt-out options.
- **Website & Digital Platforms (rafflesmumbai.com)**
    - Data entered into website contact/enquiry forms.
    - Technical data such as IP address, browser type, device details, approximate location, and cookie identifiers, in line with the website's cookie practices.
- **Corporate Governance & Legal Records**
    - Board and shareholder information, legal agreements, compliance and regulatory filings, internal approvals.
- **Accounting-related Data**
    - Billing and invoicing details, payment records, transaction information, tax-related data (where required), reimbursement documents, and financial audit references that may include personal identifiers.
- **Vendor, Consultant & Partner Data**
    - Contact details of vendors / consultants, bank details for payment, contractual agreements, performance records.
- **Employment & HR Records**
    - Employee personal data in HR files and systems.
- **Storage on Microsoft Teams / SharePoint / Other Collaboration Tools**
    - Contracts, legal papers, vendor records and related documents stored in controlled teams channels and OneDrive folders.

7. Principles of Data Processing

RMB adheres to the following principles:

1. **Lawfulness, Fairness & Transparency**
    - Provide clear notices to individuals explaining what data is collected, why, and how it will be used.
    - Avoid deceptive or misleading data practices.
2. **Purpose Limitation**
    - Use personal data only for the specified purposes communicated at the time of collection or as permitted by law.
3. **Data Minimisation**
    - Collect only data that is adequate, relevant and limited to what is necessary.
4. **Accuracy**
    - Take reasonable steps to ensure data is accurate and up-to-date.
    - Provide mechanisms for Data Principals to request correction of inaccurate or incomplete data.
5. **Storage Limitation**
    - Retain personal data only for as long as necessary for the specified purpose, legal requirements, or legitimate business needs.
    - Implement secure deletion or anonymisation after the retention period.
6. **Integrity & Confidentiality (Security)**
    - Protect data using appropriate technical and organisational measures to prevent unauthorised access, alteration, disclosure or destruction.
7. **Accountability**
    - Maintain documentation and evidence of compliance.
    - Conduct periodic reviews and audits where necessary.

8. Data Principal Rights and How We Respond

Under the DPDP framework, Data Principals are entitled to several rights. RMB will establish processes to ensure that individuals can exercise these rights effectively, including:

1. **Right to Access**
    - To obtain confirmation whether their personal data is being processed and to access such data in a reasonable format.

2. **Right to Correction and Completion**
    - To request correction of inaccurate or incomplete personal data.
3. **Right to Erasure**
    - To request erasure of personal data that is no longer necessary for the specified purpose or where consent is withdrawn, subject to legal retention obligations.
4. **Right to Withdraw Consent**
    - To withdraw consent at any time, without affecting the lawfulness of processing done prior to withdrawal.
5. **Right to Grievance Redressal**
    - To raise grievances regarding data processing and receive a response within the timelines prescribed by the DPDP Act/Rules.
6. **Right to Nominate**
    - To nominate another individual who can exercise rights in case of death or incapacity, where the law so provides.

Timelines:
We will respond to Data Principal requests within the timeframes required under the DPDP Rules (currently envisaged as within 90 days for rights requests and within 72 hours for reporting notifiable breaches to the Data Protection Board, where applicable).

9. Consent Management

- RMB shall maintain clear consent records, including when, how, and for what purpose consent was obtained.
- Consent requests will be presented in clear and plain language, separate from other terms where feasible.
- Mechanisms will be in place to enable easy withdrawal of consent (for example, unsubscribe links in emails, email requests, forms, or self-service portals, where available).

10. Data Security Measures

RMB will implement appropriate security controls, including but not limited to:

- **Access Control**
    - Role-based access to systems and folders containing personal data.
    - Access granted on "need-to-know" basis and revoked upon exit or role change.
- **Technical Controls**
    - Use of secure passwords, Two factor authentication where feasible, device encryption, secure network configurations.
    - Security hardening of Microsoft 365, Teams, and other collaboration platforms.

- **Data in Transit and at Rest**
    - Use of encryption and secure communication protocols for data transfers where appropriate.
    - Regular backups stored securely and subject to retention/deletion controls.
- **Physical Security (where applicable)**
    - Restricted access to offices, server rooms, and physical files that may contain personal data.
- **Monitoring and Logging**
    - Logging of access and changes to critical systems containing personal data, as feasible.
- **Training & Awareness**
    - Periodic training for all relevant staff on DPDP requirements, phishing awareness, secure handling of data, and incident reporting.

11. Cross-Border Data Transfers

Personal data may be transferred outside India (To global Raffles group entities or to cloud servers located abroad) only:

- Where such transfer is not prohibited under any notification of the Central Government; and
- Subject to appropriate contractual and security safeguards ensuring that the personal data continues to receive a reasonable level of protection.

12. Data Retention and Deletion

RMB will maintain a Data Retention Schedule specifying how long different categories of data are retained

Broadly:

- **Student and academic records** – retained for the duration of the programme plus a defined number of years for alumni references, legal/regulatory requirements, and accreditation.
- **Vendor and contract records** – retained for the term of the contract plus limitation periods for legal claims.
- **Employee records** – retained for the period of employment plus a specified time post-separation, as legally required.
- **Website logs and analytics data** – retained only as long as necessary for security, analytics and troubleshooting.

When data is no longer required, it will be securely deleted, anonymised, or irreversibly de-identified in accordance with internal procedures.

13. Personal Data Breach Management

RMB maintains a breach response mechanism including:

1. **Detection and Internal Reporting**
    - Any employee who becomes aware of a potential breach must immediately report it to IT Security and the Data Protection Lead / DPO.
2. **Containment and Assessment**
    - Prompt action to secure systems, limit further unauthorised access, and determine the nature, scope and impact of the breach.
3. **Notification to Data Protection Board and Data Principals**
    - Where the breach is assessed as notifiable under DPDP Rules (e.g. likely to cause significant harm), RMB will notify the Data Protection Board as soon as practicable and no later than the time limits prescribed (currently, guidance indicates within 72 hours of becoming aware).
    - Affected Data Principals will also be informed without undue delay, in clear, plain language.
4. **Remediation and Documentation**
    - Implementation of remedial measures to prevent recurrence.
    - Maintenance of an incident register, documenting causes, actions taken, and outcomes.

14. Website and Cookies (RMB)

The RMB website (rafflesmumbai.com) may collect:

- Information actively provided by users via forms (name, contact details, programme interest, location, etc.)
- Technical information such as IP address, device type, browser, and usage patterns.
- Cookies or similar technologies for functionality, analytics and (if implemented) marketing.

The site will:

- Present a clear Privacy / Data Protection Notice and, where relevant, a cookie notice/consent banner.
- Allow users to contact RMB for questions or to exercise their rights.

15. Governance, Review and Updates

- This Policy will be reviewed at least once every year or sooner if:
    - There are changes in law or DPDP Rules;
    - The scope of data processing significantly changes;
    - There are material incidents or audit findings.
- Any substantial updates will be approved by the appropriate governance body and communicated to employees and, where relevant, to Data Principals (e.g., via updated privacy notices on the website).