SRI DEVAGIRI VENKATESHWARASWAMI TEMPLE TRUST

PRIVACY POLICY

This Privacy Policy explains how the Trust may collect, use, store, share and protect personal information relating to devotees, visitors, donors, pilgrims, volunteers and users of Temple services.

1. SCOPE OF THIS PRIVACY POLICY

This Privacy Policy applies, as relevant, to personal information processed in connection with visits to Sri Devagiri Venkateshwaraswami Temple, darshan arrangements, seva and pooja bookings, donations, prasadam or annadanam arrangements, accommodation or facility enquiries, festival and event registrations, feedback, complaints, telephone or email enquiries, and the Trust's official website or other digital services.

It applies to information collected directly by the Trust or by service providers acting on its behalf for an authorised Temple purpose. A particular service, event, booking or facility may provide an additional notice or specific conditions. If a separate notice applies to a particular activity, it should be read together with this Policy.

2. INFORMATION THE TRUST MAY COLLECT

Depending on the service used and the information needed to provide it, the Trust may collect a person's name, mobile number, email address, postal address, age or date of birth where relevant, preferred language, and other contact details voluntarily provided.

For darshan, seva, pooja, event or accommodation arrangements, the Trust may collect booking date, selected service, number of participants, devotee or participant names, booking reference, special requests and communication history. The Trust should collect only details reasonably needed for the relevant arrangement.

For donations and payments, the Trust may maintain donor name and contact details, donation amount, date, payment method, transaction reference, receipt details and any information voluntarily supplied for acknowledgement or accounting purposes. Complete card numbers, UPI PINs, passwords and one-time passwords should not be requested or stored by the Trust.

The Trust may also receive information when a person submits a feedback form, complaint, lost-property report, accessibility request, volunteer enquiry or other communication.

3. BOOKING AND DEVOTEE SERVICE INFORMATION

When a devotee books or enquires about darshan, seva, pooja, accommodation, annadanam or an event, the Trust may use the submitted information to check availability, confirm the request, manage attendance, communicate schedule changes, verify a booking and maintain appropriate administrative records.

Where a booking is made on behalf of another person or group, the person submitting the details should have the authority or permission needed to provide those details. The person making the booking should ensure that names, contact details, dates and service selections are accurate.

Information about religious participation or a requested service may be personal in nature. The Trust should limit access to such information to authorised persons who need it to administer the relevant service.

4. DONATION AND CONTRIBUTION INFORMATION

When a person makes or enquires about a donation, the Trust may process details needed to identify and record the contribution, issue an acknowledgement or receipt, reconcile the payment, maintain accounts, respond to donor queries and meet applicable legal or audit requirements.

Where a donor requests a receipt in a particular name or provides details for a specific lawful purpose, the Trust may record those details as required. Donors should avoid including unnecessary sensitive personal information in donation references or enquiry messages.

Donation information may be retained for accounting, audit, financial reporting, dispute resolution and other lawful recordkeeping purposes. A donation does not, by itself, authorise the Trust to publish a donor's name or contribution publicly. Any public acknowledgement should follow the donor's stated preference and the Trust's approved practice.

5. TECHNICAL AND WEBSITE INFORMATION

If the Trust operates a website, booking portal or other digital service, the system or its hosting provider may automatically record technical information such as IP address, browser type, device type, operating system, access date and time, pages or functions accessed, referral information, error reports and security events.

Such information may be used to operate the website, maintain availability, troubleshoot errors, understand service usage, prevent misuse, protect accounts and investigate security incidents. The actual information collected will depend on the website configuration and tools enabled by the Trust.

6. COOKIES AND SIMILAR TECHNOLOGIES

The Trust's website may use cookies or similar technologies where enabled. These may support essential functions such as session management, security, language or preference settings, booking workflows and website performance.

If analytics, embedded maps, social-media features or other third-party tools are used, those services may set or read their own cookies or collect technical information under their respective privacy notices. Where applicable law requires a notice or choice for non-essential cookies, the Trust should provide an appropriate mechanism.

Users may be able to manage cookies through their browser settings. Disabling certain cookies may affect the operation of some website features or booking functions.

7. HOW THE TRUST MAY USE INFORMATION

The Trust may use information for the following purposes, where relevant and lawful:

- To respond to questions, requests, complaints and feedback from devotees and visitors.
- To administer darshan, seva, pooja, event, accommodation and other service bookings.
- To process donations, reconcile payments, issue receipts and maintain financial records.
- To communicate confirmations, reminders, schedule changes, safety instructions and service updates.
- To manage crowd arrangements, access controls, lost-property matters and visitor assistance.
- To maintain the security, availability and proper functioning of Temple premises and digital systems.
- To maintain records required for administration, accounting, audit, legal compliance and dispute resolution.
- To detect or investigate suspected fraud, misuse, unauthorised access or other security concerns.
- To improve the clarity, accessibility and operation of Temple services, based on appropriate and proportionate information.

8. PURPOSE AND LAWFUL BASIS OF PROCESSING

The Trust intends to collect and use personal information for clear, specific and legitimate Temple or Trust purposes. Depending on the activity and applicable law, processing may be based on an individual's consent, a request made by that individual, the steps needed to provide a requested service, compliance with legal obligations, protection of legitimate interests where legally permitted, or another lawful basis.

Where consent is relied upon, the Trust should explain the purpose and provide a suitable way to give or withdraw consent. Withdrawal of consent will not necessarily affect processing already carried out lawfully before withdrawal. It may also mean that the Trust cannot continue a service that requires the relevant information.

9. SHARING OF INFORMATION

The Trust does not intend to sell personal information as part of its ordinary Temple administration. Information may be shared only where reasonably necessary for an identified purpose, authorised by the individual, required by law or otherwise permitted under applicable law.

Depending on the activity, recipients may include authorised Trust office-bearers and personnel, priests or service coordinators who need relevant booking details, accounting or audit professionals, banks and payment processors, website or hosting providers, messaging or email providers, security and technology vendors, legal advisers, and government or regulatory authorities where legally required.

The Trust should limit the information shared to what the recipient reasonably needs and, where appropriate, use contractual or other safeguards to require service providers to protect the information and use it only for authorised purposes.

10. THIRD-PARTY SERVICE PROVIDERS

The Trust may use independent providers for website hosting, booking software, payment processing, SMS or email delivery, cloud storage, security, analytics, database management or other administrative functions. These providers may process information to perform services for the Trust and may also have their own legal responsibilities and privacy notices.

Users should review the privacy information of a third-party service when they are redirected to that service or choose to interact with it directly. The Trust does not control the independent privacy practices of third-party websites or platforms.

11. INTERNATIONAL DATA PROCESSING

Some technology or communication providers may store or process information on infrastructure located outside India. Whether this occurs depends on the providers and systems actually selected by the Trust.

If personal information is processed or stored outside India, the Trust should ensure that the arrangement complies with applicable Indian law and any relevant contractual or regulatory requirements. The Trust should identify the countries or service providers involved where such disclosure is required by law or appropriate for transparency.

12. CHILDREN'S INFORMATION

Children may visit the Temple with parents, guardians or other responsible adults. The Trust should avoid collecting children's personal information unless it is reasonably required for a specific Temple purpose, such as a booking, event registration, safety matter or response to an enquiry.

Where applicable law requires parental or guardian consent or additional safeguards for a child's personal information, the Trust should implement those requirements before collecting or using the information. Adults submitting information about a child should ensure that they are authorised to do so.

The Trust should not knowingly use children's information for unrelated promotional purposes. Any photograph, video or other identifiable information involving children should be handled with particular care and in accordance with applicable law and the Trust's approved practices.

13. SENSITIVE OR CONFIDENTIAL INFORMATION

Individuals should not submit sensitive personal information unless it is genuinely necessary for the relevant request and the Trust has provided an appropriate authorised channel. Unnecessary medical, financial, identity or other confidential details should not be included in general enquiry forms or public messages.

If a person voluntarily provides information about a health, accessibility or assistance requirement, the Trust should use it only to assess or provide the requested assistance and restrict access to personnel who need it for that purpose, subject to applicable law.

14. DATA RETENTION

The Trust should retain personal information only for as long as reasonably necessary for the purpose for which it was collected, taking account of service administration, financial and accounting records, audit, security, legal obligations, dispute resolution and other lawful requirements.

Different categories of information may require different retention periods. Booking details, donation receipts, accounting records, enquiry correspondence, technical logs and security records may therefore be retained for different periods depending on their purpose and applicable requirements.

When information is no longer required, the Trust should take reasonable steps to securely delete it, anonymise it or otherwise dispose of it in an appropriate manner, unless retention is required or permitted by law.

15. INFORMATION SECURITY

The Trust should use reasonable technical, physical and organisational safeguards appropriate to the nature of the information and the systems used. Depending on actual facilities and technology, safeguards may include restricted access to paper records, secure storage, password-protected accounts, role-based access, secure website connections, system updates, backups, access logs and staff or volunteer instructions.

Access to personal information should be limited to authorised persons who need it for their assigned responsibilities. Records should not be left unattended in public areas or shared through personal accounts or unauthorised channels.

No website, electronic transmission, storage system or physical recordkeeping arrangement can be guaranteed completely secure. Individuals should use official contact and payment channels and should not disclose passwords, PINs, OTPs or other authentication credentials.

16. DATA INCIDENTS AND BREACH MANAGEMENT

If the Trust becomes aware of a suspected loss, unauthorised disclosure, alteration, destruction or access involving personal information under its responsibility, it should take appropriate steps to assess and address the incident.

Depending on the nature and seriousness of the incident, response steps may include restricting access, securing affected systems or records, preserving relevant evidence, investigating the cause, taking corrective action and notifying affected individuals or authorities where required by applicable law.

Individuals who believe that their information has been exposed, misused or sent to an incorrect recipient should contact the Trust through its verified official privacy or grievance channel and provide relevant details without sending passwords, PINs or OTPs.

17. INDIVIDUAL PRIVACY RIGHTS AND REQUESTS

Subject to applicable law and the circumstances of processing, individuals may have rights or mechanisms to request information about the processing of their personal data, seek access to or correction of inaccurate information, request updating or erasure where legally available, withdraw consent where processing is based on consent, and raise a grievance.

The Trust may need to verify the identity or authority of the person making a request before responding, especially where the request concerns donation, booking, financial or other confidential records. Requests made on behalf of another person may require proof of authority.

Some information may need to be retained to meet legal, accounting, audit, security or dispute-resolution requirements. Where a request cannot be fully met, the Trust should explain the reason to the extent required by applicable law.

18. WITHDRAWAL OF CONSENT

Where the Trust processes information on the basis of consent, an individual may withdraw that consent through the method made available by the Trust or by contacting the designated privacy channel.

Withdrawal will not make earlier lawful processing invalid. It may affect the Trust’s ability to complete a booking, provide a requested facility, respond to a request or continue another activity for which the information is necessary. The Trust will explain any material service impact where appropriate.

19. CORRECTION AND UPDATING INFORMATION

Individuals should provide accurate and current information when making bookings, donations or enquiries. If a person identifies an error in information held by the Trust, they may submit a correction request through the official channel.

The Trust may ask for the relevant booking reference, receipt or reasonable verification before changing a record. Certain financial or statutory records may need to be corrected through a documented process rather than overwritten or deleted.

20. DELETION AND ERASURE REQUESTS

Individuals may request deletion of personal information where such a right is available under applicable law. The Trust will consider the request in light of the purpose for which the information was collected and any legal or operational requirement to retain it.

Information may need to be retained for accounting, audit, statutory compliance, security, fraud prevention, legal claims or dispute resolution. Where deletion is not possible, the Trust should restrict use to the purposes for which retention is required, where appropriate and legally permitted.

21. COMMUNICATIONS AND SERVICE NOTICES

The Trust may use the contact details supplied by an individual to send booking confirmations, donation acknowledgements, receipts, schedule changes, event information requested by the individual, safety notices, responses to enquiries and other service-related communications.

If the Trust sends optional promotional or general updates, it should provide an appropriate way to opt out where required by law. Essential messages relating to an active booking, transaction, security matter or requested service may still be sent where necessary.

Individuals are responsible for providing a correct mobile number or email address and for updating it when it changes. The Trust cannot ensure delivery where contact details are incorrect or a third-party network or email provider fails.

22. PAYMENT INFORMATION

Online payments, where offered, may be processed by an independent bank, payment gateway, UPI provider, card network or other financial service. The payment provider may collect and process payment credentials directly under its own terms and privacy practices.

The Trust may receive transaction-related information such as payment status, amount, date, reference number, payer details made available by the provider and receipt information. The Trust should not ask users to send full card details, UPI PINs, passwords or OTPs by email, phone, message or website form.

If a payment is unsuccessful, duplicated or appears incorrect, the individual should contact the Trust and, where appropriate, the payment provider using verified contact details. Transaction references may be requested to investigate the issue.

23. CCTV, PHOTOGRAPHY AND SECURITY RECORDS

If CCTV or other security recording systems are operated at Temple premises, recordings may be used for visitor safety, crowd management, protection of property, incident investigation and other lawful security purposes. The Trust should display appropriate notices where required and restrict access to recordings to authorised personnel.

Retention and disclosure of any security recording should follow the Trust's actual security procedures and applicable law. Individuals should not assume that every area is recorded or that footage will always be available. This section applies only to the extent that such systems are in fact used by the Trust.

Photography or video recording by visitors is subject to Temple rules and any restrictions in particular areas. The Trust's privacy obligations concerning information it controls are separate from the responsibilities of individuals who independently take or publish photographs.

24. EXTERNAL LINKS AND EMBEDDED SERVICES

The Temple website or digital communications may contain links to external websites, maps, payment pages, social-media platforms or other services. Those services are operated independently and may have their own privacy notices, security measures and data practices.

Before providing personal information on an external website or platform, users should check that they are using the intended service and review its privacy information. The Trust is not responsible for the privacy practices of independently operated services, subject to any responsibility imposed by applicable law.

25. VOLUNTEER, STAFF AND SERVICE PROVIDER INFORMATION

If the Trust invites applications or registrations from volunteers, staff, priests, contractors or service providers, it may process contact details, role preferences, qualifications or experience where relevant, availability, identification or verification details where lawfully required, and communications relating to the application or engagement.

Such information should be used for the relevant selection, administration, verification, coordination, safety or engagement purpose and retained only for an appropriate period, subject to applicable legal and recordkeeping requirements.

26. LEGAL AND REGULATORY DISCLOSURES

The Trust may disclose information where required by applicable law, a lawful request or order of a competent authority, or where reasonably necessary to protect the safety of individuals, prevent fraud or misuse, investigate an incident, enforce applicable terms or establish, exercise or defend legal rights.

Where legally permitted and reasonably practicable, the Trust should limit disclosures to the information required for the relevant purpose and maintain appropriate records of such disclosures.

27. DIGITAL PERSONAL DATA PROTECTION AND APPLICABLE LAW

The Trust intends to handle digital personal data in accordance with applicable Indian data-protection and privacy requirements, including the Digital Personal Data Protection Act, 2023 and rules or provisions to the extent they are in force and apply to the relevant processing activity.

The exact obligations depend on the Trust's role, the type of information, the purpose of processing, the systems used and the legal requirements in force at the relevant time. The Trust should obtain legal advice to confirm its notices, consent processes, grievance arrangements, retention practices and other compliance steps before publication.

28. PRIVACY GRIEVANCES AND CONTACT

Individuals may raise privacy questions, requests or complaints through the Trust's verified official communication channels. A request should clearly state the issue and include relevant information, such as a booking reference or receipt number, where necessary. Do not include passwords, PINs or OTPs.

Before publication, the Trust should insert and verify its designated privacy or grievance contact, official email address, telephone number, postal or registered office address and official website address. These details must be controlled by the Trust and kept current.

Privacy / Grievance Contact: To be designated by the Trust.
Official Email: To be inserted and verified.
Telephone: To be inserted and verified.
Registered / Correspondence Address: To be inserted and verified.
Official Website: To be inserted and verified.

29. CHANGES TO THIS PRIVACY POLICY

The Trust may revise this Policy to reflect changes in Temple activities, booking facilities, website features, service providers, information-handling practices, security measures or applicable law.

The latest version should display its effective or updated date and be made available through the official Temple website or another appropriate channel. Where a material change requires notice or consent under applicable law, the Trust should provide the required notice or obtain the required consent.

30. PRIVACY COMMITMENT

The Trust aims to follow principles of transparency, purpose limitation, data minimisation, appropriate access, reasonable security, responsible retention and lawful use of personal information. Information entrusted to the Trust should be handled with care and used only for legitimate Temple, devotee-service, administrative or legal purposes.

All persons authorised to handle personal information on behalf of the Trust should be given appropriate instructions about confidentiality, secure handling, permitted use and reporting of suspected incidents.