

PRAKRTIREVA SARANAM FOUNDATION

DATA PROTECTION & PRIVACY POLICY

Policy Version: 1.0

Effective Date: 27 August 2026

Approved By: Board of Directors

Approval Date: 27 August 2026

Policy Owner: Board of Directors

Privacy Contact: _____

Email: _____

Next Review Date: 27 August 2027

1. PURPOSE

Praktireva Saranam Foundation (“the Foundation”, “PSF”, “we”, “us” or “our”) is committed to respecting and protecting the privacy and personal information of individuals who interact with the Foundation.

The Foundation may collect and process personal information in connection with its volunteer programmes, plantation drives, school activities, environmental awareness programmes, website, events, donations, communications, reimbursement processes and other organisational activities.

This Data Protection & Privacy Policy (“Policy”) establishes the principles and practices that the Foundation follows when collecting, using, storing, sharing, protecting and disposing of personal information.

The purposes of this Policy are to:

- promote responsible handling of personal information;
 - protect individuals against inappropriate use or disclosure of their information;
 - establish clear responsibilities for handling personal information;
 - provide transparency about the information collected by the Foundation;
 - establish appropriate safeguards for sensitive and child-related information;
 - provide mechanisms for privacy-related requests and concerns; and
 - support compliance with applicable data-protection and privacy laws.
-

2. SCOPE

2.1 This Policy applies to personal information handled by the Foundation in connection with its activities.

2.2 It applies to information relating to:

- volunteers;
- directors and representatives;
- donors;
- supporters;
- beneficiaries;
- students and children participating in or encountered during Foundation activities;
- parents or guardians where applicable;
- school representatives;
- partner organisations;
- vendors and service providers;
- event participants;
- website visitors and users of online forms; and
- other individuals who communicate or interact with the Foundation.

2.3 This Policy applies to personal information collected through:

- the Foundation website;
- Google Forms and other online forms;
- email and other authorised communication channels;
- volunteer registration and onboarding;
- school/site survey processes;
- plantation drives and Foundation programmes;
- reimbursement and expense processes;
- events and activities;
- photographs and videos;
- donations and supporter interactions; and
- other authorised Foundation activities.

3. DEFINITIONS

For the purposes of this Policy:

3.1 Personal Information

“Personal information” means information relating to an identified or identifiable individual.

Examples may include:

- name;
- phone number;
- email address;
- residential or correspondence details;
- identification information;
- photographs;
- videos;
- bank/payment information;
- volunteer records;
- communication records; and
- other information that can identify an individual.

3.2 Personal Data

Where applicable, “personal data” has the meaning assigned to it under applicable data-protection law.

3.3 Processing

Processing may include collecting, recording, organising, storing, using, sharing, transferring, updating or deleting personal information.

3.4 Data Principal

Where applicable under the Digital Personal Data Protection Act, 2023 (“DPDP Act”), an individual to whom personal data relates is referred to as a “Data Principal”.

3.5 Data Fiduciary

Where applicable under the DPDP Act, the person or organisation that determines the purpose and means of processing personal data is referred to as a “Data Fiduciary”.

4. PRIVACY PRINCIPLES

The Foundation seeks to handle personal information according to the following principles:

4.1 Purpose Limitation

Personal information should be collected for specified and legitimate organisational purposes.

4.2 Data Minimisation

The Foundation should seek to collect only information reasonably necessary for the relevant purpose.

4.3 Accuracy

Reasonable steps should be taken to keep personal information accurate and appropriately updated.

4.4 Security

Appropriate organisational and technical safeguards should be used to protect personal information.

4.5 Confidentiality

Personal information should not be disclosed unnecessarily or accessed by unauthorised persons.

4.6 Retention Limitation

Personal information should not be retained longer than reasonably necessary for the purpose for which it was collected, subject to legal, accounting, regulatory or legitimate organisational requirements.

4.7 Accountability

Persons authorised to handle personal information are expected to follow this Policy and applicable procedures.

5. TYPES OF INFORMATION THE FOUNDATION MAY COLLECT

Depending on the nature of the interaction, the Foundation may collect:

5.1 Volunteer Information

- name;
- age or date of birth where required;
- contact information;
- educational or professional information where relevant;
- location or city/state information;
- emergency contact information;
- volunteer interests and skills;

- onboarding information;
- declarations and acknowledgements; and
- information reasonably required to assess suitability for particular volunteer activities.

5.2 Reimbursement Information

For authorised reimbursement purposes, the Foundation may collect:

- expense details;
- receipts;
- travel information;
- bank account information;
- payment details; and
- other information necessary to process an approved reimbursement.

5.3 School and Programme Information

The Foundation may collect information relating to:

- schools;
- school representatives;
- programme coordinators;
- site survey information;
- activity participants;
- programme photographs and videos; and
- other information required to organise Foundation activities.

5.4 Donor and Supporter Information

Depending on the interaction, this may include:

- name;
- contact details;
- donation information;
- transaction information;
- communication preferences; and
- information required for applicable records or reporting.

5.5 Website and Technical Information

The Foundation's website or digital services may collect certain technical information such as:

- IP address;
- browser or device information;
- website usage information;
- approximate location information where technically available;
- cookies or similar technologies where used; and

- information voluntarily submitted through website forms.
-

6. HOW INFORMATION IS COLLECTED

The Foundation may collect personal information:

- directly from the individual;
- through authorised Foundation forms;
- through Google Forms or similar digital forms;
- through email;
- during volunteer onboarding;
- during school visits and surveys;
- during Foundation programmes and events;
- through the Foundation website;
- from authorised partner organisations;
- from schools or institutions where appropriate; or
- through other lawful and authorised means.

The Foundation should seek to provide appropriate information or notice regarding the purpose for which personal information is being collected.

7. PURPOSES OF PROCESSING

Personal information may be used for legitimate Foundation purposes including:

- volunteer registration and onboarding;
- communication with volunteers;
- organising plantation drives;
- conducting school visits and surveys;
- coordinating events and programmes;
- maintaining volunteer records;
- processing authorised reimbursements;
- maintaining financial and accounting records;
- communicating with donors and supporters;
- responding to enquiries;
- maintaining website and digital services;
- safeguarding children and other participants;
- preventing misuse or fraud;
- maintaining organisational records;
- complying with applicable legal requirements;
- responding to complaints and concerns; and

- other purposes communicated to the individual or otherwise permitted by applicable law.
-

8. LEGAL BASIS FOR PROCESSING

The Foundation shall process personal information only for lawful and appropriate purposes.

Depending on the circumstances and applicable law, processing may be based on:

- consent;
- a legal obligation;
- a legitimate organisational or legally recognised purpose;
- contractual or administrative necessity;
- protection of an individual's safety or interests; or
- another lawful basis available under applicable law.

Where consent is required, the Foundation shall seek consent in an appropriate manner.

The Foundation shall comply with applicable requirements of the DPDP Act and related Rules as and when the relevant provisions become applicable to the Foundation.

9. NOTICE AND TRANSPARENCY

Where personal information is collected directly from an individual, the Foundation should provide appropriate information about:

- what information is being collected;
- why it is being collected;
- how it may be used;
- relevant third parties or service providers where applicable;
- applicable rights and choices; and
- how privacy-related concerns can be raised.

Information should be communicated in clear and reasonably understandable language.

10. CONSENT

10.1 Where consent is required, the Foundation shall seek consent through an appropriate mechanism.

10.2 Consent should be informed and linked to the purpose for which personal information is being collected.

10.3 An individual should not be asked to provide unnecessary personal information merely as a condition for participating in an unrelated Foundation activity.

10.4 Where applicable law provides a right to withdraw consent, the Foundation shall provide an appropriate mechanism for doing so.

10.5 Withdrawal of consent may not affect processing that the Foundation is otherwise legally permitted or required to undertake.

11. VOLUNTEER DATA

11.1 Volunteer information shall be used primarily for legitimate volunteer-management and Foundation-related purposes.

11.2 Volunteers should not be given access to another volunteer's personal information unless such access is necessary and authorised.

11.3 Volunteer contact information should not be publicly disclosed without appropriate authorisation.

11.4 Volunteers shall not copy, download, forward, publish or otherwise misuse personal information obtained through Foundation activities.

11.5 Access to volunteer records shall be restricted according to role and organisational need.

12. CHILDREN'S PERSONAL INFORMATION

The Foundation recognises that information relating to children requires particular care.

12.1 The Foundation shall seek to handle children's personal information in accordance with applicable child-protection, privacy and data-protection requirements.

12.2 The Foundation shall avoid collecting unnecessary personal information about children.

12.3 Volunteers shall not independently collect or retain personal information about students unless authorised for a legitimate Foundation purpose.

12.4 Where consent or other authorisation is required for the collection or use of children's information, the Foundation shall follow the applicable requirements.

12.5 Children's information shall not be used for unrelated personal purposes.

12.6 The Foundation's **Child Safeguarding & Protection Policy** shall also apply to information and activities involving children.

13. PHOTOGRAPHS AND VIDEOS

13.1 Photographs and videos may be collected during Foundation activities for legitimate organisational purposes such as:

- documenting activities;
- maintaining programme records;
- reporting to stakeholders;
- educational and awareness purposes;
- Foundation communications; and
- social-media or website content where appropriately authorised.

13.2 Photography and videography involving children shall be handled in accordance with the Foundation's Child Safeguarding & Protection Policy and applicable consent or authorisation requirements.

13.3 Volunteers shall not use photographs or videos taken during Foundation activities for unrelated personal or commercial purposes without appropriate authorisation.

13.4 Volunteers should not upload or distribute sensitive or inappropriate images involving participants.

13.5 The Foundation may restrict or remove content where a privacy, safeguarding or other legitimate concern arises.

14. SOCIAL MEDIA AND PUBLICATION

14.1 Personal information, photographs or videos obtained through Foundation activities shall not be published through personal social-media accounts without appropriate authorisation.

14.2 Foundation-related content intended for public publication should follow the Foundation's authorised communication process.

14.3 Volunteers shall not disclose:

- confidential information;
- private contact information;
- personal documents;
- complaint details;
- sensitive safeguarding information; or
- other protected information

through public platforms.

14.4 The Foundation may maintain official social-media accounts and may publish authorised programme content in accordance with applicable privacy and consent requirements.

15. DATA SHARING AND DISCLOSURE

The Foundation may share personal information where reasonably necessary with:

- authorised Foundation personnel;
- schools or institutions involved in a programme;
- professional advisers;
- auditors or accountants;
- payment or banking service providers;
- website and technology service providers;
- form, cloud-storage or productivity service providers;
- government or regulatory authorities where legally required;
- emergency or competent authorities where necessary for safety; or
- other authorised parties for legitimate organisational purposes.

The Foundation shall seek to limit disclosure to information reasonably necessary for the relevant purpose.

16. THIRD-PARTY SERVICE PROVIDERS

The Foundation may use third-party services to support its operations.

These may include services for:

- website hosting;
- cloud storage;
- Google Forms and Google Sheets;
- email;
- analytics;
- payment processing;
- communication;
- website maintenance;
- social-media management; and
- other operational functions.

Where third-party services process personal information on behalf of the Foundation, the Foundation should seek to use reasonable safeguards and appropriate contractual or organisational arrangements where appropriate.

Individuals should also understand that third-party services may have their own privacy terms and practices.

17. GOOGLE FORMS, SHEETS AND CLOUD STORAGE

17.1 The Foundation may use Google Forms, Google Sheets, Google Drive or similar cloud services for legitimate organisational purposes.

17.2 Access to personal information stored in such systems should be restricted to authorised persons.

17.3 Sensitive information should not be placed in publicly accessible documents or spreadsheets.

17.4 Sharing permissions should be reviewed periodically.

17.5 Forms should collect only information reasonably necessary for their stated purpose.

17.6 Response spreadsheets should not be shared through unrestricted public links.

17.7 When a volunteer or team member no longer requires access, their access should be removed promptly.

18. ACCESS CONTROL

18.1 Access to personal information shall be provided according to organisational role and legitimate need.

18.2 Persons with access shall:

- use information only for authorised purposes;
- protect account credentials;
- avoid sharing passwords;
- avoid downloading unnecessary copies;
- avoid storing information on insecure devices where reasonably avoidable; and
- report suspected unauthorised access.

18.3 Access permissions for Foundation systems should be reviewed periodically.

19. INFORMATION SECURITY

The Foundation shall seek to implement reasonable technical and organisational safeguards appropriate to the nature and sensitivity of the information handled.

Depending on the circumstances, safeguards may include:

- password protection;
- access controls;
- restricted sharing permissions;
- secure cloud storage;
- device security;
- account authentication;
- limited access to sensitive records;
- appropriate backups;
- secure deletion; and
- staff or volunteer awareness.

No digital system can be guaranteed to be completely secure. The Foundation shall nevertheless take reasonable steps to reduce foreseeable privacy and security risks.

20. DATA BREACHES AND SECURITY INCIDENTS

A privacy or security incident may include:

- unauthorised access;

- accidental disclosure;
- loss of a device containing personal information;
- unauthorised sharing;
- compromised accounts;
- accidental deletion or alteration; or
- other events that may compromise personal information.

Any person who becomes aware of a suspected privacy or security incident should report it promptly to:

Privacy Contact: _____

Email: _____

Phone: _____

The Foundation shall assess the incident and take appropriate action, including notification or reporting where required by applicable law.

21. DATA RETENTION

21.1 The Foundation shall seek to retain personal information only for as long as reasonably necessary for the relevant purpose or as required by applicable law.

21.2 Different categories of information may need to be retained for different periods.

21.3 Records may need to be retained for purposes including:

- accounting and financial records;
- statutory or regulatory compliance;
- legal claims or disputes;
- volunteer administration;
- programme documentation;
- safeguarding records;
- audit requirements; and
- organisational history.

21.4 When personal information is no longer required, the Foundation should securely delete, destroy or anonymise it where reasonably practicable and appropriate.

22. ACCURACY AND CORRECTION

The Foundation seeks to maintain accurate personal information.

Individuals may request correction of inaccurate or incomplete information relating to them through the Foundation's designated privacy contact.

Where appropriate, the Foundation may request sufficient information to verify the identity of the requester before making changes.

23. ACCESS TO PERSONAL INFORMATION

Subject to applicable law and reasonable verification requirements, individuals may contact the Foundation to request information regarding personal data held about them.

Where applicable under the DPDP Act and relevant provisions in force, the Foundation shall provide rights and mechanisms required by law.

Requests should be directed to:

Privacy Contact: _____

Email: _____

24. ERASURE / DELETION REQUESTS

An individual may request deletion or erasure of personal information where such a right is available under applicable law.

The Foundation may retain information where retention is required or permitted for:

- legal compliance;
 - financial or accounting requirements;
 - safeguarding;
 - legal claims;
 - dispute resolution;
 - fraud prevention; or
 - other legitimate purposes permitted by applicable law.
-

25. GRIEVANCE REDRESSAL

Individuals who have concerns regarding the Foundation's handling of personal information may contact the designated privacy contact.

The Foundation shall seek to review and respond to privacy-related grievances within the applicable legal or organisational timeframe.

Privacy / Grievance Contact: _____

Email: _____

Phone: _____

Where applicable, individuals shall retain any statutory rights to approach the competent authority or mechanism established under applicable law.

26. CONFIDENTIALITY

Persons authorised to access personal information are expected to maintain confidentiality.

Personal information shall not be:

- discussed unnecessarily;
- disclosed to unauthorised persons;
- published publicly without appropriate authority;
- used for personal benefit; or
- retained after access is no longer required, subject to applicable retention requirements.

Confidentiality obligations may continue after a person stops volunteering or working with the Foundation.

27. VOLUNTEER RESPONSIBILITIES

Every Foundation volunteer who handles personal information shall:

- respect privacy;
- access information only when authorised;
- use information only for legitimate Foundation purposes;
- keep information confidential;

- follow applicable Foundation policies;
 - protect devices and accounts used for Foundation work;
 - avoid unnecessary copying or downloading;
 - report suspected privacy incidents; and
 - return, delete or appropriately dispose of Foundation information when their authorised role ends.
-

28. DIRECTOR AND MANAGEMENT RESPONSIBILITIES

The Board of Directors and authorised management representatives shall seek to:

- establish appropriate privacy practices;
 - maintain this Policy;
 - restrict access to personal information;
 - provide appropriate guidance to volunteers;
 - respond to privacy concerns;
 - review significant security incidents;
 - maintain appropriate records; and
 - update privacy practices when applicable legal or operational requirements change.
-

29. PRIVACY BY DESIGN AND DATA MINIMISATION

When creating a new Foundation form, programme, website feature or data-collection process, the Foundation should consider:

- whether the information is actually necessary;
- why the information is required;
- who will have access;
- how long it needs to be retained;
- whether the same purpose can be achieved with less information;
- whether children are involved;
- whether consent or another lawful basis is required; and
- what safeguards should be applied.

The Foundation should avoid collecting personal information merely because a form can technically collect it.

30. WEBSITE PRIVACY

The Foundation's website may contain:

- contact forms;
- volunteer registration forms;
- donation facilities;
- links to external services;
- analytics tools;
- cookies or similar technologies; and
- downloadable documents.

The Foundation shall seek to provide appropriate information regarding data collection through relevant website notices or forms.

External websites linked from the Foundation's website may operate under their own privacy policies and terms.

31. COOKIES AND ANALYTICS

Where the Foundation uses cookies, analytics or similar technologies, they may be used for purposes such as:

- website functionality;
- security;
- understanding website usage;
- improving website performance; and
- measuring communication effectiveness.

The Foundation shall seek to implement appropriate notices, controls and consent mechanisms where required by applicable law.

32. DATA TRANSFERS AND EXTERNAL PROCESSING

Personal information may be processed or stored using service providers whose infrastructure may be located in India or another jurisdiction.

The Foundation shall handle such processing in accordance with applicable legal requirements and any restrictions applicable to the relevant data.

Where applicable law imposes requirements relating to transfer of personal data outside India, the Foundation shall follow those requirements.

33. DATA RELATING TO DONORS AND FINANCIAL TRANSACTIONS

The Foundation may retain information relating to donations and financial transactions for legitimate accounting, audit, reporting, tax, regulatory and organisational purposes.

Payment card, banking or other financial information processed through an external payment provider may also be subject to that provider's security and privacy practices.

The Foundation shall not request unnecessary financial information through general volunteer or public forms.

34. DATA RELATING TO SAFEGUARDING AND COMPLAINTS

Information relating to:

- child-safeguarding concerns;
- sexual-harassment complaints;
- misconduct reports;
- disciplinary matters; and
- other sensitive complaints

shall receive appropriate confidentiality and access restrictions.

Such information shall be handled in accordance with the Foundation's relevant policies, including the **Child Safeguarding & Protection Policy**, **Volunteer Code of Conduct**, and **POSH & Safe Workplace Policy**, as applicable.

35. INFORMATION RECEIVED FROM SCHOOLS AND PARTNERS

Where the Foundation receives personal information from a school, institution, partner organisation or other authorised source, the Foundation shall use that information only for appropriate and authorised purposes.

The Foundation shall seek to avoid unnecessary onward disclosure.

Where responsibilities for personal information are shared between organisations, the Foundation shall seek to clarify the relevant responsibilities where reasonably necessary.

36. INTERNATIONAL AND EXTERNAL SERVICE PROVIDERS

The Foundation may use technology and service providers that operate internationally.

Examples may include:

- cloud-storage providers;
- website hosting providers;
- email providers;
- analytics providers;
- communication platforms; and
- other digital service providers.

Use of such providers does not remove the Foundation's responsibility to apply reasonable privacy and security practices to information under its control.

37. POLICY BREACHES

A breach of this Policy may result in appropriate organisational action.

Depending on the circumstances, action may include:

- guidance or counselling;
- additional training;
- restriction of access;
- removal from a particular responsibility;

- suspension of volunteer access;
- termination of volunteer engagement; or
- referral to appropriate authorities where required.

Serious breaches involving unlawful disclosure, misuse of personal information, fraud, harassment, safeguarding concerns or other misconduct may be dealt with under the Foundation's other applicable policies and procedures.

38. REPORTING A PRIVACY CONCERN

Any person who believes that their personal information has been:

- improperly collected;
- unnecessarily disclosed;
- accessed without authorisation;
- misused;
- lost;
- compromised; or
- otherwise handled inappropriately

should report the concern promptly.

Privacy Contact: _____

Email: _____

Phone: _____

The Foundation shall seek to assess and respond to genuine privacy concerns appropriately.

39. RELATIONSHIP WITH OTHER FOUNDATION POLICIES

This Policy should be read together with the Foundation's other applicable policies and procedures, including:

- **Volunteer Code of Conduct**
- **Child Safeguarding & Protection Policy**
- **POSH & Safe Workplace Policy**
- **Volunteer Reimbursement Policy**

- Volunteer Registration and Onboarding requirements
- applicable website terms and notices
- other policies or procedures introduced by the Foundation

Where another Foundation policy provides additional protection for a particular category of information or person, the additional requirements shall also apply.

Where applicable law imposes a higher or different requirement, the applicable law shall prevail.

40. POLICY REVIEW AND ADMINISTRATION

40.1 This Policy shall be maintained under the Foundation's document-control system.

40.2 The Policy shall be reviewed periodically and when significant changes occur in:

- applicable law;
- Foundation activities;
- technology;
- data-collection practices;
- website functionality; or
- organisational structure.

40.3 Amendments shall be made through the Foundation's authorised approval process.

40.4 The latest approved version shall be maintained as the official version.

40.5 Previous versions shall be appropriately archived and shall not be represented as the current Policy.

41. DATA PROTECTION ACKNOWLEDGEMENT

I acknowledge that I have been provided access to the **Praktireva Saranam Foundation Data Protection & Privacy Policy**.

I understand that when handling personal information in connection with Foundation activities, I am expected to:

- respect individuals' privacy;
- access personal information only when authorised;
- use information only for legitimate Foundation purposes;
- maintain confidentiality;
- protect Foundation information and accounts;
- avoid unauthorised sharing or publication;
- follow applicable Foundation policies; and
- report suspected privacy or security incidents promptly.

I understand that violation of this Policy may result in appropriate organisational action.

Name: _____

Role / Volunteer ID (if applicable): _____

Signature: _____

Date: _____

42. DOCUMENT CONTROL

Policy Name: Data Protection & Privacy Policy

Organisation: Prakrtireva Saranam Foundation

Policy Version: 1.0

Effective Date: 27 August 2026

Approval Date: 27 August 2026

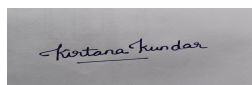
Approved By: Board of Directors

Policy Owner: Board of Directors

Privacy Contact: _____

Next Review Date: 27 August 2027

Authorised Signature:



Name & Designation: Kirtana Kunder – Director