

PRAKRTIREVA SARANAM FOUNDATION

A Section 8 Company

CONFIDENTIALITY POLICY

Policy Number: PSF/VP/CONF/01

Version: 1.0

Effective Date: 02 September 2026

Approval Date: 02 September 2026

Approved By: Board of Directors

Policy Owner: Praktireva Saranam Foundation

1. PURPOSE

Praktireva Saranam Foundation is committed to protecting confidential information entrusted to it by volunteers, directors, interns, consultants, partners, schools, donors, beneficiaries, community members and other stakeholders.

The purpose of this Confidentiality Policy is to establish clear standards for identifying, handling, using, storing and sharing confidential information obtained through or in connection with the Foundation's activities.

This policy aims to ensure that confidential information is:

- Treated responsibly and respectfully;
- Accessed only when necessary for legitimate Foundation purposes;
- Protected against unauthorized access, disclosure, misuse, loss or alteration;
- Shared only with authorized persons where there is a legitimate need or appropriate basis;
- Handled appropriately during and after a person's association with the Foundation.

Maintaining confidentiality is essential to protecting individual privacy, maintaining trust and safeguarding the integrity and reputation of the Foundation.

2. POLICY STATEMENT

Praktireva Saranam Foundation expects everyone acting on its behalf or participating in its activities to maintain appropriate confidentiality.

No person covered by this policy shall disclose, misuse, copy, distribute, publish or otherwise make confidential Foundation information available to an unauthorized person.

Confidential information must be handled carefully regardless of whether it is received:

- Verbally;
- In writing;
- Electronically;
- Through photographs or videos;
- Through documents or records;
- Through digital platforms;
- During meetings or discussions; or
- Through participation in Foundation activities.

Confidentiality obligations apply during a person's association with the Foundation and may continue after their association ends where information remains confidential or where disclosure would be inappropriate or unlawful.

The Foundation will take reasonable measures to protect confidential information and expects everyone covered by this policy to cooperate with these measures.

3. SCOPE

This policy applies to all persons who receive, access, handle or become aware of confidential information through their association with Praktireva Saranam Foundation, including:

- Directors;
- Board members;
- Volunteers;
- Interns;
- Consultants;
- Advisors and representatives;
- Committee members;
- Project coordinators;
- Persons assisting with Foundation activities; and
- Any other person authorized to access confidential Foundation information.

This policy applies to information obtained through or in connection with:

- Plantation drives;
- School and community activities;
- Environmental programmes;

- Volunteer activities;
 - Meetings and discussions;
 - Foundation documents and records;
 - Email and other communication channels;
 - Google Drive, Google Forms, spreadsheets and other digital systems;
 - Social media and content creation activities;
 - Photographs and videos;
 - Donor and partner interactions; and
 - Other Foundation-related activities.
-

4. DEFINITION OF CONFIDENTIAL INFORMATION

For the purpose of this policy, **Confidential Information** means information that is not intended for public disclosure and that a person knows, or reasonably should know, must be kept private or protected.

Confidential information may include, but is not limited to:

4.1 Personal Information

- Names and contact details;
- Phone numbers and email addresses;
- Addresses and other identifying information;
- Volunteer registration information;
- Personal documents submitted to the Foundation;
- Emergency contact information;
- Information relating to individual circumstances.

4.2 Child-Related Information

Information relating to children participating in or encountered during Foundation activities, including:

- Names and contact information;
- Photographs and videos where privacy restrictions apply;
- Personal or family information;
- Safeguarding concerns or reports;
- Complaints or incidents involving children; and
- Information that could identify a child in a sensitive context.

Child-related information must also be handled in accordance with the Foundation's **Child Safeguarding & Protection Policy**.

4.3 Donor and Financial Information

- Donor information;
- Donation records;
- Bank or transaction-related information;
- Financial records not intended for public disclosure;
- Internal budgets;
- Expense and reimbursement information where personal or sensitive; and
- Other non-public financial information.

4.4 Internal Organizational Information

- Internal discussions;
- Confidential meeting records and minutes;
- Internal decisions before public announcement;
- Draft policies and documents;
- Internal reports;
- Operational plans;
- Unpublished project information; and
- Internal communications.

4.5 Volunteer and Team Information

- Volunteer applications and registration information;
- Personal information shared by volunteers;
- Internal volunteer discussions;
- Complaints, grievances or concerns;
- Conduct-related information;
- Disciplinary information; and
- Other private team matters.

4.6 Partner and School Information

- Information provided confidentially by schools;
 - Partner or collaborator information;
 - Internal communications with partner organizations;
 - Information received under an expectation of confidentiality; and
 - Sensitive information relating to programme locations or activities.
-

5. CONFIDENTIALITY PRINCIPLES

Everyone covered by this policy should follow the following principles:

5.1 Need-to-Know Principle

Confidential information should only be accessed or shared when it is reasonably necessary for a legitimate Foundation-related purpose.

5.2 Minimum Necessary Information

Only the information reasonably necessary for the relevant task should be accessed, used or shared.

5.3 Responsible Handling

Confidential information must be handled carefully and protected from accidental or unauthorized disclosure.

5.4 Respect for Privacy

Everyone must respect the privacy and dignity of individuals whose information they access through Foundation activities.

5.5 No Personal Use

Confidential Foundation information must not be used for personal benefit, commercial purposes, personal disputes or any other unauthorized purpose.

5.6 Appropriate Disclosure

Confidential information may only be disclosed when authorized, required for a legitimate Foundation purpose, consented to where appropriate, or otherwise permitted or required by applicable law.

6. RESPONSIBILITIES

6.1 Directors and Board Members

Directors and Board members are responsible for:

- Promoting a culture of confidentiality;
- Protecting confidential organizational information;

- Ensuring appropriate access controls;
- Handling sensitive matters responsibly;
- Taking appropriate action when a confidentiality concern is reported; and
- Supporting compliance with this policy.

6.2 Volunteers

Volunteers must:

- Protect confidential information they access;
- Use information only for authorized Foundation activities;
- Avoid sharing confidential information with unauthorized persons;
- Keep passwords and access credentials secure;
- Follow Foundation instructions regarding photographs, documents and digital information;
- Report suspected confidentiality breaches promptly; and
- Continue to respect confidentiality after their volunteering ends.

6.3 Interns, Consultants and Representatives

Interns, consultants and representatives must follow the same confidentiality standards applicable to their role and must not disclose Foundation information outside the scope of their authorization.

7. HANDLING CONFIDENTIAL INFORMATION

Confidential information must be handled responsibly.

Persons covered by this policy should:

- Keep confidential documents secure;
 - Avoid leaving confidential documents unattended;
 - Use Foundation-approved or authorized communication channels where available;
 - Verify recipients before sending sensitive information;
 - Avoid forwarding confidential messages unnecessarily;
 - Avoid storing sensitive information on shared or unsecured devices;
 - Protect passwords and account credentials;
 - Use appropriate privacy settings when handling digital information; and
 - Dispose of confidential information securely when it is no longer required.
-

8. DIGITAL CONFIDENTIALITY

When using digital systems, everyone must take reasonable precautions to protect confidential information.

This includes:

- Using strong and unique passwords;
- Not sharing passwords or login credentials;
- Not allowing unauthorized persons to access Foundation accounts;
- Locking devices when unattended;
- Avoiding access to confidential information through insecure or unauthorized devices where reasonably avoidable;
- Checking email recipients before sending sensitive information;
- Not uploading confidential information to unauthorized websites, applications or services;
- Not using confidential Foundation information for personal AI tools or other external services unless authorized; and
- Reporting suspected unauthorized access promptly.

Foundation files and records stored in services such as Google Drive, Google Forms, spreadsheets or other platforms must only be accessed by persons who have been appropriately authorized.

9. PHOTOGRAPHS, VIDEOS AND SOCIAL MEDIA

Photographs and videos taken during Foundation activities may contain personal or sensitive information.

Persons covered by this policy must therefore:

- Follow Foundation instructions regarding photography and filming;
- Respect applicable consent and privacy requirements;
- Avoid photographing or recording sensitive situations unnecessarily;
- Not share private or sensitive photographs or videos through personal accounts without authorization;
- Not publish confidential information in captions, comments, stories, posts or videos;
- Not disclose private details about volunteers, children, schools, donors or partners; and
- Follow the Foundation's **Child Safeguarding & Protection Policy** when children are involved.

Publicity or social media content should only contain information that is appropriate and authorized for public communication.

10. CHILDREN AND SAFEGUARDING INFORMATION

Information relating to children requires particular care.

Any safeguarding concern, complaint, allegation, incident or other sensitive information involving a child must be treated as confidential.

Persons must not:

- Discuss safeguarding concerns casually with others;
- Share identifying information about a child unnecessarily;
- Post details about safeguarding incidents online;
- Forward safeguarding complaints or reports to unauthorized persons; or
- Attempt to investigate or resolve serious safeguarding concerns outside the Foundation's established process.

Safeguarding information should only be shared with the appropriate authorized persons on a need-to-know basis.

The **Child Safeguarding & Protection Policy** must be followed alongside this policy.

11. DONOR, VOLUNTEER AND PARTNER INFORMATION

The Foundation respects the confidentiality of information provided by donors, volunteers, schools, partners and other stakeholders.

Such information must not be disclosed for personal, commercial or unrelated purposes.

Examples include:

- Donor contact details;
- Volunteer personal information;
- Private school information;
- Partner contact information;
- Private communications;

- Personal circumstances; and
- Non-public project information.

Publicly available information is not automatically confidential; however, individuals should exercise reasonable judgment before combining or sharing information in a manner that could compromise someone's privacy.

12. INTERNAL COMMUNICATIONS

Internal Foundation communications may contain information that is not intended for public distribution.

Persons covered by this policy must not:

- Forward confidential internal emails unnecessarily;
- Share screenshots of private discussions;
- Publish internal disagreements;
- Distribute confidential meeting discussions;
- Share draft decisions before authorization; or
- Use internal communications to embarrass, threaten or harm another person.

Internal disagreements should be addressed through appropriate Foundation channels.

13. MEETINGS AND DOCUMENTS

Confidential information discussed during Foundation meetings must be treated appropriately.

Meeting participants should:

- Avoid discussing confidential matters in public places where they may be overheard;
- Keep confidential documents secure;
- Share meeting materials only with authorized participants;
- Avoid recording meetings without appropriate authorization; and
- Ensure confidential meeting notes are not publicly circulated.

Official meeting minutes and records should be maintained according to the Foundation's applicable governance and record-keeping practices.

14. PERMITTED DISCLOSURE

Confidential information may be disclosed where:

1. The disclosure is authorized by the Foundation;
2. The recipient has a legitimate need to know the information;
3. The individual concerned has provided appropriate consent, where applicable;
4. Disclosure is necessary for an authorized Foundation activity;
5. Disclosure is required or permitted by applicable law or a lawful authority; or
6. Disclosure is necessary to protect a person from serious harm or to address a safeguarding or safety concern.

Where uncertain, the person should seek guidance from the appropriate Foundation authority before disclosing the information.

15. PROHIBITED DISCLOSURE

Unless authorized or otherwise permitted under this policy, persons covered by this policy must not:

- Share confidential information with friends or family;
 - Share confidential information through personal social media accounts;
 - Publish private information online;
 - Forward confidential emails unnecessarily;
 - Share screenshots of private Foundation conversations;
 - Copy or remove confidential records for personal use;
 - Sell or commercially exploit confidential information;
 - Use confidential information for personal advantage;
 - Discuss confidential matters in public places; or
 - Provide confidential information to media or external organizations without authorization.
-

16. CONFIDENTIALITY AFTER VOLUNTEERING OR ASSOCIATION ENDS

Confidentiality responsibilities do not automatically end when a person's volunteering, consultancy, internship, directorship, advisory role or other association with the Foundation ends.

After leaving the Foundation, individuals must not use or disclose confidential information obtained through their previous association for unauthorized purposes.

Where appropriate, individuals may be required to return or securely delete Foundation documents, files, records or other confidential information in their possession.

17. THIRD-PARTY CONFIDENTIAL INFORMATION

The Foundation may receive confidential information from schools, donors, partners, consultants, community members or other organizations.

Such information must be respected and handled according to any applicable confidentiality obligations or restrictions.

Foundation personnel must not assume that information received from a third party can automatically be shared internally or externally.

Where there is uncertainty, guidance should be sought before disclosure.

18. REPORTING A CONFIDENTIALITY CONCERN OR BREACH

Anyone who becomes aware of a suspected or actual confidentiality breach should report it promptly through the Foundation's appropriate reporting channel.

Examples of potential breaches include:

- Sending confidential information to the wrong person;
- Losing a device containing confidential information;
- Unauthorized access to Foundation files;
- Sharing private information on social media;
- Unauthorized disclosure of donor or volunteer information;
- Sharing sensitive child-related information;
- Unauthorized copying or downloading of confidential documents; or
- Suspected misuse of confidential information.

Reports should be made in good faith and should contain as much relevant information as reasonably possible.

19. RESPONSE TO CONFIDENTIALITY BREACHES

When a potential breach is reported, the Foundation may take appropriate steps depending on the circumstances.

These may include:

- Assessing the nature and extent of the breach;
- Restricting or removing access;
- Securing affected information;
- Requesting deletion or return of improperly shared information;
- Informing affected persons where appropriate;
- Taking safeguarding or safety measures where necessary;
- Maintaining appropriate records;
- Taking corrective or preventive action; and
- Taking disciplinary or other appropriate action where warranted.

Where required, the Foundation may also take steps in accordance with applicable legal or regulatory requirements.

20. NON-RETALIATION

The Foundation does not support retaliation against a person who raises a confidentiality concern or reports a suspected breach in good faith.

Anyone who raises a genuine concern should not be subjected to harassment, intimidation, discrimination or other adverse treatment merely because they made the report.

Knowingly making false or malicious allegations may, however, be addressed appropriately.

21. EXCEPTIONS

This policy does not prevent appropriate disclosure where disclosure is:

- Authorized by the Foundation;
- Required by applicable law;
- Required by a lawful order or competent authority;
- Necessary to address a serious safety or safeguarding concern; or
- Otherwise permitted under an applicable Foundation policy or procedure.

Where possible, the person should seek guidance before making a disclosure.

22. TRAINING AND AWARENESS

The Foundation may provide appropriate guidance or training to persons who handle confidential information.

Persons covered by this policy are expected to:

- Read and understand this policy;
 - Follow applicable confidentiality procedures;
 - Ask for clarification when uncertain;
 - Participate in relevant awareness or training activities where required; and
 - Report concerns promptly.
-

23. RECORD KEEPING

The Foundation will maintain appropriate records relating to confidentiality matters where necessary.

Records may include:

- Reports of suspected breaches;
- Actions taken in response;
- Relevant communications;
- Access or security records where available;
- Corrective measures; and
- Other documentation necessary for organizational, safeguarding, legal or compliance purposes.

Confidential records must themselves be handled securely and accessed only by authorized persons.

24. RELATIONSHIP WITH OTHER POLICIES

This policy should be read together with other relevant Foundation policies, including:

- Data Protection & Privacy Policy;
- Child Safeguarding & Protection Policy;
- Volunteer Code of Conduct;
- Volunteer Safety Guidelines;
- Inclusion & Non-Discrimination Policy;
- Grievance Redressal Policy;
- Conflict of Interest Policy;
- Anti-Fraud & Anti-Corruption Policy; and
- Other applicable Foundation policies and procedures.

Where another policy contains more specific requirements relating to a particular type of information or situation, those requirements should also be followed.

25. BREACH OF THIS POLICY

Failure to comply with this policy may result in appropriate action depending on the nature and seriousness of the breach.

Depending on the circumstances, action may include:

- Guidance or counselling;
- Additional training;
- Restriction or removal of access to Foundation information;
- Removal from a particular activity or role;
- Termination of volunteer or other association;
- Recovery or deletion of improperly retained information; or
- Other appropriate action consistent with applicable law and Foundation procedures.

Serious matters may also be referred to the appropriate authority where required.

26. POLICY REVIEW

This policy will be reviewed periodically to ensure that it remains relevant, effective and aligned with the Foundation's activities and applicable requirements.

The Foundation may revise this policy when necessary due to:

- Changes in law or regulatory requirements;
- Changes in organizational activities;
- Changes in technology or information systems;
- Lessons learned from incidents or reviews; or
- Changes in best practices.

The Board of Directors or authorized governing authority will approve material revisions to the policy.

27. ACKNOWLEDGEMENT

All persons covered by this policy are expected to read, understand and follow the Confidentiality Policy.

Where the Foundation requires an acknowledgement, the individual may be asked to confirm that they:

- Have read and understood this policy;
- Agree to maintain confidentiality;
- Will use confidential information only for authorized purposes;
- Will not disclose confidential information without authorization; and
- Will promptly report suspected confidentiality breaches.

Acknowledgement may be obtained through the Foundation's volunteer onboarding process, policy acknowledgement form, electronic confirmation or other appropriate method.

28. CONTACT AND REPORTING

For questions or guidance regarding confidentiality, individuals should contact the Foundation through its official communication channels.

General Contact: info@praktirevasaranam.org

Volunteer Matters: volunteers@praktirevasaranam.org

Director / Governance Matters: director@praktirevasaranam.org

For reporting a grievance, safeguarding concern or other issue, individuals should use the appropriate reporting mechanism established by the Foundation.

29. APPROVAL AND AUTHORIZATION

This Confidentiality Policy has been approved by the Board of Directors of Praktireva Saranam Foundation.

Policy: Confidentiality Policy

Version: 1.0

Effective Date: 02 September 2026

Approval Date: 02 September 2026

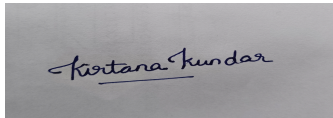
Approved By: Board of Directors

Board Approval

Name: Kirtana Kundar

Designation: Director / Authorized Board Member

Signature:



Date: 02 September 2026

DOCUMENT CONTROL

Version	Effective Date	Description	Approved By
1.0	02 September 2026	Initial policy	Board of Directors

END OF POLICY