



Confidentiality Policy

FPMT Regional Office North America Inc. (“FPMT-RONA”) is committed to maintaining high standards in the area of confidentiality. We respect the right to privacy and confidentiality of those who have contact with FPMT-RONA. This policy gives guidance for ensuring confidentiality and outlines the circumstances where disclosures may be necessary.

Employees and volunteers must protect all confidential information, including donor records, employee data, and internal communications. Confidentiality agreements may be required depending on role and access level.

Confidential information includes all personal, sensitive and identifying information about individuals. Information about an individual should not be shared without the consent of the individual concerned.

There are, however, circumstances where personal information may be required to be passed on to the appropriate person such as the Designated Protection Person or to external agencies or authorities:

1. Protecting from Abuse

If a concern regarding abuse is expressed to a member of staff who is not an FPMT-RONA Designated Protection Person (DPP), that staff member will share that concern with an FPMT-RONA DPP, in order to enable the DPP to take it forward, as described in our Protecting from Abuse Policy.

Once a concern regarding abuse is raised or an allegation is made, both the alleged victim and the alleged perpetrator are entitled to have confidentiality until they are able and willing to have the information in the public realm. However, these are the circumstances when information must be disclosed, even if the alleged victim or perpetrator are not ready to consent to disclosure.

Circumstances When Information Must be Disclosed:

a) FPMT-RONA staff or board members may need to share sensitive information in order to take practical steps to protect the person at risk and the community:

- If the individual is under 18 and they disclose information that may indicate risk to themselves or other children or young people;
- If an adult discloses past child abuse and it is possible that children or young people are currently at risk from the abuser;

- If they believe that the individual/s involved is imminently intent on an act of self-harm or of significant harm to another person;
- If they believe that the person has committed an act of harm or abuse to him/herself or to another person either recently or at some time in the past;
- Where there is any other safeguarding issue to be dealt with in line with our Protecting from Abuse Policy;
- If the participant gives information that indicates that a crime has been committed;
- Where a person is receiving medical care from others (including for mental health issues) or is receiving counselling from another organization, there may be some sharing of information where it is deemed appropriate and beneficial to the person involved. The person will be informed of any such sharing of information.
- The individual/s gives information that indicates a possible terrorist threat.

b) Statutory and Legal Responsibilities:

- As FPMT-RONA staff and volunteers work in different states and possibly different countries, they abide by the statutory and legal requirements of the state/country in which they reside. If there is a statutory or legal requirement to inform the local authority and other relevant agencies to ensure protection from significant harm or abuse, information will be provided as required.

c) Responsibility to Fellow Affiliates:

- The FPMT-RONA Designated Protection Person/s may inform other FPMT regional and national coordinators, and any FPMT center directly impacted, of any serious safeguarding issues and action taken, in order to enable them to protect local community members from the risk of harm and abuse.
- It is FPMT Inc. policy that all concerns regarding abuse relating to an affiliate board member, director, or spiritual program coordinator, or an FPMT registered, resident, or Tibetan teacher, must be reported to the Center Services and/or Teacher Services director (who are also Designated Protection People) at FPMT International Office.
- Additionally, if the allegation is regarding an ordained person, the information must be shared with the director of the FPMT Sangha body, the International Mahayana Institute, so they can ensure that Vinaya is upheld.

If information needs to be disclosed:

- If a decision has to be taken to break confidentiality, it will be done only after consultation with a Designated Protection Person.
- The person/s involved will be informed that the disclosure they are making may not be kept confidential.
- Any such disclosure will be shared internally or with external agencies as required while respecting the person's privacy as much as possible.

- Such sharing will only include those who need to know and the information necessary to ensure that the person is protected from harm and abuse and that proper processes are followed if they have been harmed.

Anonymized sharing of information:

- If FPMT-RONA believes that information regarding a complaint or concern must be shared within the FPMT community, in order to inform regarding lessons needing to be learnt, and to allow people to discuss in a way that fosters understanding and community healing, we will anonymize the people involved.
- For FPMT-RONA board review: anonymized information on all safeguarding incidents will be provided to the board to enable the board to fulfil their safeguarding responsibilities. The board will manage and minimize the risk of further incidents happening as far as this is reasonably possible, by supporting any necessary changes to policies, procedures and work practices.

2. Data Privacy Policy

This policy pertains to the following website: www.fpmtna.org.

FPMT Regional Office North America Inc. (“we,” “us,” or “our”) is a 501(c)(3) non-profit organization registered in the United States. We respect your privacy and are committed to protecting your personal information. This Privacy Policy explains how we collect, use, disclose, and safeguard your data when you interact with our website www.fpmtna.org (the “Site”), including through our contact form.

Information We Collect

We collect the following personal information only when you voluntarily submit it via our contact form:

- Name (first and/or last name you provide)
- Email address
- Message content (your inquiry or feedback)

We also automatically collect:

- IP address
- Browser type and version
- Date and time of submission
- Referring page (if applicable)

How We Use Your Information

We use the collected data solely for:

- Responding to your inquiry or message
- Improving our services and website functionality

- Internal record-keeping and compliance with IRS non-profit reporting
- Preventing spam, fraud, or abuse

We do NOT sell, rent, or trade your personal information with third parties for marketing purposes.

Legal Basis (CCPA, CalOPPA & GDPR Compliance)

CCPA (California residents): We collect minimal PII for a legitimate business purpose (responding to contact requests).

GDPR (EU/UK residents): Processing is based on your consent (provided when submitting the form) and legitimate interest (answering your message).

Data Sharing & Disclosure

We may share your data only with:

- Authorized staff and volunteers who need access to respond
- Service providers bound by confidentiality (e.g., Formspree, Google Workspace, or our web host) under written agreements
- Law enforcement or government authorities if required by law (e.g., subpoena)

Data Storage & Security

Storage & Processing: We collect only the minimum data needed to handle inquiries, newsletters, and website analytics. All data is stored securely with encryption and full GDPR compliance:

- Contact form (name, email, message): Sent via email to office@fpmtna.org and stored in Google Workspace (Gmail) — encrypted at rest (AES-256) and in transit (TLS), hosted in Google data centers (EU/US regions with GDPR DPA/SCCs). Deleted after processing your inquiry.
- Newsletter signup (email): Stored in Constant Contact (US servers, GDPR-compliant via SCCs), encrypted (AES-256 at rest, TLS in transit). Used solely for sending emails with easy unsubscribe. Export/deletion on request.
- Website analytics (anonymized IP, cookies, visit data): Stored in Matomo (self-hosted on our US servers), encrypted at rest (AES-256) and in transit (TLS). Configured for GDPR (IP masking, consent tools, data retention). Used only for site improvement; no personal identification.
- We do not share data with third parties except as required to deliver services (see Google DPA, Constant Contact privacy, and Matomo GDPR tools).
- Learn more: [Google Workspace DPA](#) | [Constant Contact Privacy](#) | [Matomo GDPR](#)

Retention: We retain contact form data only as long as necessary to process your inquiry, then permanently delete unless required longer for legal purposes.

Security: We use HTTPS, encryption, access controls, and regular security reviews.

Cookies & Tracking

Our site uses only essential cookies (if any) to make the contact form work. We do not use analytics, advertising, or tracking cookies unless explicitly stated here.

If we add Google Analytics or similar in the future, we will update this policy and display a cookie banner.

Your Rights

You have the right to:

- Access your data
- Correct inaccurate data
- Delete your data (“right to be forgotten”)
- Opt-out of future communications
- Non-discrimination for exercising your rights

To exercise these rights, email us at: office@fpmtna.org

California residents: You may submit a verifiable request under CCPA. We will respond within 45 days.

Children’s Privacy (COPPA)

Our Site is not directed to children under 13. We do not knowingly collect data from children. If we learn we have, we will delete it immediately.

Changes to This Policy

We may update this Privacy Policy. Changes will be posted here with a new “Effective Date.” We will notify you via email if changes are material.

Contact Us

For questions about this policy: Email: office@fpmtna.org

Sending us an Email

Individuals may decide to send us personally identifying information, for example, in an email message containing a question or comment, or by filling out a Web form that provides us this information. We use personally identifying information from email primarily to respond to requests. We may forward emails to other employees who are better able to answer questions. We may also use emails to contact them in the future about our programs that may be of interest.

If an individual signs up for one of our email lists, we will only send the kinds of information they have requested. We won’t share names or email addresses with any outside parties.