

MASHAL DATA PROTECTION POLICY



Mashal
20-c, Patliputra Colony, Patna,
Bihar

FOREWORD BY THE PRESIDENT

In an era where data is power, Mashal reaffirms its unwavering commitment to safeguarding the personal information entrusted to us by the individuals, communities, and partners we work with. This *Data Protection Policy* reflects our strong resolve to protect privacy, promote transparency, and ensure ethical handling of data across all our operations.

The policy aligns with national legislation, including the Digital Personal Data Protection Act, 2023, and draws from international best practices. It provides clear procedures and responsibilities to guide our staff, partners, and stakeholders in collecting, processing, storing, and sharing personal data.

Let this policy be a living document—informing decisions, reinforcing accountability, and enhancing trust with the communities we serve. I encourage all team members to read, understand, and apply this policy diligently in their daily work.

With responsibility and foresight,



Sister Mary Alice,

President, Mashal

Date: 12.07.2025

1. Purpose and Scope

The purpose of this policy is to establish clear guidelines for the collection, processing, storage, transmission, and disposal of personal data handled by Mashal. This policy applies to:

- All employees, volunteers, consultants, interns, and contractors.
- All programs, projects, and operations of Mashal.
- All data—physical or digital—relating to individuals, communities, donors, beneficiaries, staff, and partners.

2. Definitions

Personal Data: Any information relating to an identified or identifiable individual (e.g., name, address, phone number, identification numbers, photographs, bank details).

Sensitive Personal Data: Includes financial information, health records, biometric data, caste/religion, sexual orientation, and political beliefs.

Processing: Any operation performed on personal data, including collection, storage, retrieval, use, transmission, and deletion.

Data Subject: An individual whose personal data is collected or processed by Mashal.

Data Protection Officer (DPO): The designated officer responsible for ensuring compliance with data protection laws and this policy.

3. Principles of Data Protection

- Lawfulness, Fairness, and Transparency – Data will be processed lawfully, fairly, and in a transparent manner.
- Purpose Limitation – Data will be collected only for specific, legitimate purposes and not used for unrelated activities.
- Data Minimization – Only the minimum necessary personal data will be collected.
- Accuracy – Data will be kept accurate and up-to-date.
- Storage Limitation – Data will be retained only for as long as necessary to fulfill the purpose.
- Integrity and Confidentiality – Data will be secured against unauthorized access, loss, or damage.
- Accountability – All staff are responsible for compliance.

4. Rights of Individuals

Mashal will uphold the rights of individuals under the Digital Personal Data Protection Act, 2023:

- Right to Access – Individuals may request access to their personal data.
- Right to Rectification – Individuals can request correction of inaccurate or incomplete data.

- Right to Erasure – Individuals can request deletion of their data when it is no longer necessary.
- Right to Withdraw Consent – Consent can be withdrawn at any time.
- Right to Data Portability – Individuals may request their data in a machine-readable format.
- Right to Object – Individuals can object to processing for certain purposes.

Requests will be addressed within 30 days.

5. Data Collection and Processing

- Consent: Written or digital consent must be obtained before collecting personal data, except where permitted by law.
- Source of Data: Data will be collected directly from individuals wherever possible.
- Processing Records: All programs must maintain a record of what data is collected, its purpose, and storage details.
- Third Parties: Any sharing of data with partners or vendors must be governed by a signed Data Processing Agreement.

6. Data Storage and Security

- Physical Records: Stored in locked cabinets with restricted access.
- Digital Records: Protected with strong passwords, encryption, and regular backups.
- Access Control: Role-based access will be enforced; no unauthorized personnel may access personal data.

Retention Schedule:

- Beneficiary records – 7 years
- Financial records – as per statutory requirement
- HR records – during employment + 5 years after
- After expiry, data will be securely destroyed.

7. Data Transmission

- Internal Transfer: Only via secure platforms (encrypted email, password-protected files).
- External Sharing: Allowed only with prior authorization and signed agreements.
- International Transfer: Must comply with applicable cross-border data protection rules.

8. Data Breach Response

Any suspected or actual data breach must be reported to the Data Protection Officer within 24 hours. The DPO will:

1. Investigate the breach.
2. Contain and mitigate risks.
3. Notify affected individuals and authorities as required.
4. Maintain a breach incident log.

9. Roles and Responsibilities

- Board of Directors: Oversight and approval of this policy.
- President: Ensures organizational commitment and resources.
- Data Protection Officer: Monitors compliance, conducts training, and acts as a contact for data subjects.
- All Staff: Follow this policy and report violations.
- IT Department: Implement and maintain digital security measures.

10. Policy Implementation

- Training: All staff will undergo annual data protection training.
- Monitoring: Regular audits will be conducted to assess compliance.
- Review: This policy will be reviewed every two years or earlier if laws change.

11. Violations and Disciplinary Action

Any breach of this policy will result in disciplinary action, including warnings, suspension, termination, or legal action. Intentional or negligent breaches may also result in liability for damages.

12. Relationship with Other Policies

This policy should be read alongside:

- Mashal's HR Policy
- IT Policy
- Whistleblower Policy
- Child Protection Policy
- Financial Management Policy

13. Effective Date

This policy is effective from 12 July 2025 and applies to all activities thereafter.

This chapter outlines Mashal's policy and procedures as adapted from the comprehensive source document provided. It includes detailed clauses on responsibilities, rights, procedures, reporting, roles, and related measures. All staff, partners, and stakeholders are required to comply with these provisions.

This document should be read in conjunction with Mashal's HR Policy, IT Policy, Whistle Blower Policy, and other governance frameworks to ensure comprehensive compliance.

All data protection obligations described here align with the Digital Personal Data Protection Act, 2023 and other applicable laws.

1st version Approved by Governing Body of Mashal on: 12.07.2025

Valid from 12.07.2025 to 30.06.2028

Chinnamma

Chinnamma KC,

Secretary,

Mashal

