TOMORROW'S FOUNDATION

Guiding Them Until They Can

DATA PROTECTION POLICY

Tomorrow's Foundation

TOMORROW'S FOUNDATION

Data Protection Policy

1. Policy Statement

This policy affirms TF's commitment to protecting personal data entrusted by beneficiaries, staff, donors, and partners. The TF shall collect, process, store, and dispose of personal data in a secure and transparent manner, consistent with legal obligations and ethical responsibilities.

2. Scope & Applicability

This policy applies to:

- All TF staff (permanent, contractual, volunteers)
- Third-party service providers
- All forms of personal data—electronic and physical

3. Definitions

- **Personal Data**: Any information relating to an identified or identifiable individual
- **Data Principal**: Individual whose personal data is processed
- **Data Fiduciary**: TF responsible for determining the purpose and means of processing
- **Sensitive Data**: Includes health data, caste, religion, financial details, biometric data

4. Lawful Basis for Data Collection

TF shall collect data only if:

- Consent is freely and explicitly provided
- Data is required for contractual, statutory, or legal purposes
- Legitimate interests align with project delivery (e.g., student enrolment, training programs)

5. Collection, Use & Processing

- Limit data collection to specific, declared purposes

  To uphold transparency and minimize risk, the organization shall strictly limit data collection to the scope of purposes that have been explicitly declared to data subjects in advance. This includes:

- **Purpose Definition**:
  Each data collection activity must be linked to a clearly defined operational, legal, or service-related objective (e.g., onboarding, compliance verification, service delivery).

- **Collection Justification**:
  Prior to gathering any data, teams must document why each data point is necessary. For instance, collecting identification documents may be justified for age verification in compliance-sensitive roles, but not for newsletter subscriptions.
- **No Secondary Use Without Consent**:
  Data collected for one purpose (e.g., registration) must not be repurposed (e.g., marketing) without obtaining fresh, informed consent from the individual.
- **Process Controls**:
  Data collection forms, online portals, and paper-based processes shall be regularly reviewed to ensure no extraneous or non-essential data is solicited.
- **Internal Audits**:
  Periodic audits should assess whether collected data aligns with the original, approved purposes. Any deviation must trigger corrective actions, including data minimization or fresh consent workflows.
- Provide clear notices explaining:

To ensure transparency and uphold informed consent principles, all data subjects must be provided with accessible and understandable notices that include the following details:

What Data is Being Collected

The notice should specify:

- **Types of personal data** (e.g., name, contact number, address, date of birth)
- **Sensitive data** if applicable (e.g., health information, financial details, identification documents)
- **Technical data** if relevant (e.g., IP addresses, device information)

Example: "We collect your full name, date of birth, and PAN card number to verify identity for onboarding."

Purpose of Collection

Explain **why** each type of data is being collected and how it will be used. This ensures the data subject understands the relevance.

Example: "Your email address is collected to send notifications regarding training schedules and compliance updates."

Retention Duration

Mention the period for which the data will be retained, and the basis for this duration.

Example: "Your data will be retained for a period of five years post engagement or as mandated by statutory guidelines."

Withdrawal of Consent Procedure

Provide step-by-step instructions for data subjects to withdraw their consent and outline the consequences of doing so.

Example:
"To withdraw consent, please email us at [tf@tomorrowsfoundation.in] with the subject line 'Consent Withdrawal.' Upon withdrawal, access to certain services or portals may be restricted."

Ensure Data Is Not Used for Purposes Beyond Those Stated

To maintain trust, legality, and ethical handling of personal data, the organization shall uphold strict purpose limitation protocols. This means:

Adherence to Declared Intent

Once data has been collected for a specific and communicated purpose, it must only be used in service of that purpose. For example, if data is gathered to verify attendance for a training session, it cannot later be used for marketing or shared externally without explicit additional consent.

No Implicit or Assumed Reuse

Data must not be reused simply because it is available. Every new use must be justified and disclosed to the data subject. Blanket permissions or implied consent are insufficient.

Secondary Use Requires New Consent

If the organization wishes to use the data for a new purpose (e.g., research, program evaluation, or outreach), it must:

- Update its privacy notice
- Clearly communicate the new intent
- Seek fresh, informed consent from the individuals concerned

Monitoring & Controls

Regular system checks and audits should be conducted to ensure that:

- Data flows remain within the boundaries of declared use
- There are no unauthorized repurposing of data across departments, projects, or platforms

6. Data Retention & Disposal

- Retain data only as long as necessary
- Follow defined retention periods:
    - Beneficiary records: 5 years post-project
    - Staff records: 7 years post-employment
- Dispose of physical records via shredding and digital data via secure deletion tools

7. Data Security Measures

- Encrypt data at rest and in transit
- Implement role-based access controls
- Store physical records in locked cabinets

8. Third-Party Data Sharing

- Share data only under signed agreements with:
    - Research partners
    - Donors (e.g., for impact evaluations)
- Ensure third parties comply with equivalent safeguards
- Prohibit onward sharing without TF's written consent

TOMORROW'S FOUNDATION

9. Data Breach Protocol

In case of breach:

- Notify affected individuals within 72 hours
- Report incident to the Data Protection Board, if required
- Conduct internal investigation and implement corrective action
- Maintain breach documentation log

10. Rights of Data Principals

- Right to access, correct, delete their data
- Right to withdraw consent
- Right to grievance redressal via a Data Protection Officer

11. Governance & Compliance

- Appoint a **Data Manager** or designate responsible staff member
- Conduct regular staff training on data handling, consent, and breach response
- Review and update this policy annually

12. Policy Review

This policy shall be reviewed annually by the management team and updated in line with changes in legislation or operational procedures.