Data Protection & Privacy Policy

1. Introduction

Yafa Relief is committed to upholding the highest standards of data protection and privacy across all its humanitarian and administrative operations. The organization recognizes that the protection of personal information is not only a legal requirement, but also an ethical and humanitarian obligation that safeguards the dignity and rights of every individual it serves.

In the course of humanitarian work, it may be necessary to collect sensitive information about beneficiaries, staff, or partners. Yafa Relief is responsible for ensuring that such information is collected, used, and stored securely, and shared only when strictly necessary and in accordance with lawful and ethical standards.

This policy is guided by the following international frameworks:

- General Data Protection Regulation (GDPR)
- Data Protection Principles in Humanitarian Action (ICRC)
- Core Humanitarian Standard (CHS)
- ICRC / IFRC Code of Conduct for Humanitarian Organizations

2. Purpose of the Policy

This policy aims to ensure that all data collected and managed by Yafa Relief:

a- Is used strictly for legitimate humanitarian purposes.
b- Is collected ethically, lawfully, and transparently.
c- Is stored and protected using secure and controlled systems.
d- Is disclosed only when legally or operationally justified and with consent when possible.
e- Is updated or deleted once the intended purpose has been fulfilled.

3. Scope of Application

This policy applies to all data handled by Yafa Relief, including:

- Paper-based data: registration forms, field assessments, personnel files.
- Electronic data: databases, email, photographs, digital records.
- Audio-visual data: video recordings, field documentation, media interviews.

It applies to all:

- Staff, volunteers, and consultants.
- Partners, suppliers, and service contractors.
- Visitors and media representatives acting on behalf of the organization.

4. Core Data Protection Principles

a) Lawfulness & Consent

Data is collected with informed consent or when required for humanitarian necessity; individuals are informed of the purpose and use.

b) Purpose Limitation

Data is used strictly for the purpose for which it was collected (e.g., distributions, sponsorships, medical relief).

c) Data Minimization

Only the minimum data required to fulfill the operational purpose is collected.

d) Accuracy

Data is reviewed and updated regularly to ensure reliability.

e) Security & Confidentiality

Data is stored securely and accessed only by authorized personnel.

f) Storage Limitation

Data is retained only as long as necessary, then deleted or destroyed securely.

g) Transparency

Individuals are informed of their rights to access, correct, or request deletion of their data.

5. Types of Data Managed by Yafa Relief

a. Beneficiary Data:

Includes names, ages, household size, and humanitarian needs. Sensitive data (e.g., medical or protection-related details) is collected only when strictly necessary and with justified purpose.

b. Staff and Volunteer Data:

Includes identity records, contact information, employment history, and payroll records, used strictly for administrative purposes.

c. Partner and Supplier Data:

Includes contractual and financial records to ensure accountability and traceability.

d. Images and Media:

Considered personal data and may only be captured, stored, or published with written consent from the individual or legal guardian (for minors).

6. Internal Data Protection Measures

1) Secure Systems:

Strong passwords, user authentication, and encryption of sensitive files.

2) Access Control:

Data access is granted based on the “minimum necessary privilege” principle.

3) Secure Storage:

Paper files are kept in locked storage; electronic files are stored on secure servers inside or outside Palestine.

4) **Data Sharing Restrictions:**

Data may not be shared externally without risk assessment and executive authorization.

5) **Secure Disposal:**

Paper data is shredded; digital data is permanently deleted when no longer needed.

7. Child Data Protection

- No data regarding children may be collected or shared without written consent from a parent or legal guardian.
- Photos and stories of children must be reviewed to avoid disclosing identity or portraying harm or distress.
- Pseudonyms or symbolic images must be used when necessary.
- Child-related content should always reflect dignity, resilience, and hope, never pity or exploitation.

8. Individual Rights Regarding Personal Data

Every individual has the right to:

1. Know what data has been collected about them.
2. Request correction of inaccurate or outdated information.
3. Request deletion of data when no longer necessary.
4. Refuse the sharing of their data with third parties.
5. Submit a formal complaint if their data is misused.

9. Data Breach Response

If a data breach occurs:

a- **Immediate Reporting:**

Staff must notify the Data Protection Officer within 24 hours.

b- **Risk Assessment:**

Determine the type of data, number of individuals affected, and level of exposure.

c- Response Measures:

Implement containment and security actions.

d- Notification:

Affected individuals and relevant donors are informed within 72 hours.

e- Documentation:

The incident is recorded in a formal registry for institutional learning.

10. Institutional Responsibilities

a) Board of Trustees

Provides oversight and ensures ethical compliance.

b) Executive Management

Ensures technical and administrative safeguards are implemented.

c) Data Protection Officer (DPO)

Supervises data collection, storage, training, and compliance.

d) All Staff & Volunteers

Fully comply with the policy and report suspected breaches.

11. Training and Capacity Building

- Regular staff training on data protection and digital security.
- Policy orientation for all new personnel.
- Security audits every six months to ensure compliance.

12. Review and Update

- The policy is reviewed annually by the Governance and Accountability Unit.
- Updates are made to reflect legal or technological developments.
- The revised policy is approved by the Board of Trustees and shared across all branches.

13.Final Statement

Data protection is not only an administrative requirement, but a reflection of our commitment to human dignity and privacy.

At Yafa Relief, safeguarding information is part of safeguarding people.

Every protected data record is a responsibility we uphold with integrity and respect.