



OFFICE OF THE CHAIRMAN OF THE BOARD OF TRUSTEES

EXECUTIVE DIRECTIVE: Privacy and Data Protection Policy

Directive Number: TF-DIR-2026-015

Date of Issuance: May 18, 2026

Effective Date: June 1, 2026

1. PURPOSE & RATIONALE

In alignment with the Turathuna Foundation's commitment to institutional excellence, rigorous governance, and compliance with the standards required by our international partners and donors, the Board of Trustees has formally approved the **Privacy and Data Protection Policy**.

The implementation of this policy is essential to ensure that our operations remain transparent, ethically sound, and fully aligned with global best practices in cultural heritage preservation and humanitarian action.

2. MANDATORY COMPLIANCE

Pursuant to the authority vested in the Chairman of the Board of Trustees, and in accordance with the Foundation's bylaws, all personnel—including Board members, management, staff, volunteers, consultants, and implementing partners—are hereby directed to adhere strictly to the guidelines and procedures set forth in the attached policy.

3. IMPLEMENTATION & ENFORCEMENT

- **Effective Date:** This policy shall come into full force and effect starting **June 1, 2026**.
- **Responsibilities:** Department heads and Project Managers are responsible for the immediate dissemination of this policy to their respective teams and for conducting necessary training to ensure full understanding and operational alignment.
- **Compliance:** Failure to adhere to the provisions of this policy may result in disciplinary action, as outlined in the *Code of Ethics and Professional Conduct*.

4. REVIEW & UPDATES

This policy shall be subject to periodic review by the Board of Trustees to ensure its ongoing effectiveness in the face of evolving operational challenges. Any proposed amendments must be submitted to the Board for formal approval.

5. ATTACHMENTS

Attached to this directive is the full version of the **Privacy and Data Protection Policy**, which serves as the official operational guide for the Foundation.

BY ORDER OF THE BOARD OF TRUSTEES:



Lama Abboud

Chair of the Board of Trustees

Turathuna Foundation



Cc:

- Executive Director
- Finance Department
- HR Department
- Project Managers
- Central Policy Repository



EXECUTIVE DIRECTIVE: Privacy and Data Protection Policy

Directive Number: TF-DIR-2026-015

Date of Issuance: May 18, 2026

Effective Date: June 1, 2026

1. PURPOSE AND SCOPE

The Turathuna Foundation respects the privacy and dignity of all individuals associated with our mission. As an organization operating in the fields of heritage preservation, community capacity building, and cultural documentation, we frequently collect, store, and process personal and sensitive data.

The purpose of this policy is to establish a rigorous framework for the lawful, transparent, and secure handling of personal data across all Foundation projects and operations. This policy applies to all Board members, employees, volunteers, consultants, and implementing partners who handle data on behalf of the Foundation.

2. CORE DATA PROTECTION PRINCIPLES

All data collection and processing activities undertaken by the Turathuna Foundation must strictly adhere to the following core principles:

- **Lawfulness, Fairness, and Transparency:** Data must be processed legally and fairly, and individuals must be informed about how their data is being used.
- **Purpose Limitation:** Data must only be collected for specified, explicit, and legitimate project purposes (e.g., beneficiary registration, oral history archiving) and not further processed in a manner incompatible with those purposes.
- **Data Minimization:** We will only collect data that is strictly adequate, relevant, and limited to what is necessary for the project.
- **Accuracy:** Data must be accurate and kept up to date.
- **Storage Limitation:** Personal data must be kept in a form that permits identification for no longer than is necessary for the purposes of the project or legal auditing requirements.

- **Integrity and Confidentiality:** Data must be processed in a manner that ensures appropriate security against unauthorized access, loss, or destruction.

3. TYPES OF PROJECT DATA HANDLED

During the execution of our projects, the Foundation typically handles:

- **Beneficiary Data:** Names, ages, contact details, and socioeconomic backgrounds of individuals participating in programs.
- **Sensitive Cultural Data:** Oral histories, personal testimonies, and historical family archives collected during documentation projects.
- **Visual Media:** Photographs, video recordings, and audio recordings of community members, artisans, and project participants.
- **Partner and Contractor Data:** Financial and contact information for artisans, experts, and suppliers.

4. INFORMED CONSENT

Informed consent is the cornerstone of our data protection strategy.

- **Clear Explanation:** Before collecting personal data, oral histories, or taking photographs/videos, project staff must clearly explain to the individual *why* the data is being collected, *how* it will be used, and *who* it will be shared with (e.g., donor reports, social media, public exhibitions).
- **Consent Forms:** Written, signed consent forms (Media Release Forms or Data Collection Consent Forms) must be obtained for formal interviews, oral histories, and public-facing media.
- **Right to Withdraw:** Individuals have the right to withdraw their consent at any time. If consent is withdrawn, the Foundation will cease using their data and remove it from active publications where technically feasible.

5. PROTECTION OF VULNERABLE GROUPS (CHILDREN AND YOUTH)

In strict alignment with our *Safeguarding and Protection Policy*:

- **Parental Consent:** No personal data, photographs, or videos of children (under 18 years of age) may be collected or published without the explicit, documented consent of a parent or legal guardian.
- **Anonymization:** When publishing media or reports involving children, identifying details (e.g., full names, home addresses, specific school names) must be omitted or anonymized to protect the child's identity and safety.

6. DATA SECURITY AND STORAGE

The Foundation mandates strict physical and digital security measures to protect sensitive data.

- **Digital Security:** All electronic files containing sensitive personal data must be stored on secure, password-protected servers or encrypted hard drives. Access is restricted on a strict "need-to-know" basis.
- **Physical Security:** Hard copies of consent forms, beneficiary lists, and sensitive archival documents must be stored in locked filing cabinets within the Foundation's offices.
- **Device Security:** Staff and volunteers must use password protection on all Foundation laptops and mobile devices used for data collection in the field.

7. DATA SHARING AND DONOR REPORTING

The Foundation frequently reports project outcomes to international donors.

- **Anonymization for Reporting:** When sharing project statistics or impact stories with external donors or the public, personal data must be aggregated or anonymized. For example, instead of sharing a beneficiary's full name and address, reports should use pseudonyms or general demographic data (e.g., "A 35-year-old female artisan from Homs").
- **Third-Party Agreements:** If data must be shared with a third-party partner or consultant (e.g., an external evaluator), they must sign a Non-Disclosure Agreement (NDA) binding them to this Privacy Policy.

8. ORAL HISTORY AND ARCHIVAL DATA

Projects involving historical documentation and memory preservation require special care.

- **Ownership and Rights:** Interviewees participating in projects retain moral rights to their stories. They must be given the option to have their testimonies archived anonymously or placed under an embargo (not published until a specific future date) if the information is highly sensitive.
- **Digital Preservation:** Digital archives of cultural significance must be backed up redundantly to prevent data loss due to hardware failure or emergencies.

9. DATA BREACH PROTOCOL

A data breach occurs when personal data is accidentally or unlawfully destroyed, lost, altered, or accessed without authorization.

- **Immediate Reporting:** Any staff member or volunteer who suspects a data breach (e.g., a lost laptop, a hacked email account, misplaced physical files) must report it to the Foundation's Management immediately.
- **Mitigation:** Management will take immediate steps to secure the remaining data, assess the risk to the affected individuals, and, if the breach poses a high risk to their rights and freedoms, notify the affected individuals and relevant authorities as required by law.

10. POLICY REVIEW

This Privacy and Data Protection Policy will be reviewed biennially, or in response to significant changes in international data protection standards or local Syrian laws, to ensure our practices remain ethical, secure, and compliant.