# DATA PRIVACY AND CONFIDENTIALITY POLICY

**I. Introduction**

The Emmanuel Ivorgba Center (TEIC) is committed to protecting the privacy and confidentiality of all individuals whose personal information it collects, uses, and stores. This includes information pertaining to our beneficiaries, donors, staff, volunteers, partners, and other stakeholders. This Data Privacy and Confidentiality Policy outlines TEIC's commitment to safeguarding sensitive information and ensuring compliance with applicable data protection laws and regulations.

**II. Purpose and Objectives**

This policy aims to:

- **Protect Personal Information:** Ensure that all personal data collected and processed by TEIC is handled with the utmost care and security.
- **Maintain Trust and Credibility:** Build and maintain the trust of our stakeholders by demonstrating a commitment to data privacy.
- **Ensure Legal and Regulatory Compliance:** Adhere to all relevant data protection laws and regulations (e.g., GDPR if applicable, state-specific privacy laws).
- **Prevent Unauthorized Access and Disclosure:** Implement measures to prevent the accidental or intentional unauthorized access, use, disclosure, alteration, or destruction of personal data.
- **Promote Responsible Data Handling:** Establish clear guidelines for the collection, use, storage, retention, and disposal of personal information.
- **Educate Staff and Volunteers:** Ensure all individuals acting on behalf of EIC understand their responsibilities regarding data privacy and confidentiality.

**III. Scope**

This policy applies to all personal data collected, processed, or stored by The Emmanuel Ivorgba Center, regardless of the format (electronic, paper, oral) or the individual's relationship with EIC (beneficiary, donor, staff, volunteer, partner, etc.). It covers data handled by all employees, volunteers, contractors, and board members of TEIC.

**IV. Definitions**

- **Personal Data:** Any information that relates to an identified or identifiable individual. This includes, but is not limited to:

- **Direct Identifiers:** Name, address, email address, phone number, social security number, date of birth.
- **Indirect Identifiers:** IP address, cookie identifiers, location data, biometric data, unique device identifiers.
- **Sensitive Personal Data:** Information concerning race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, sexual orientation, genetic data, biometric data for the purpose of uniquely identifying an individual.

- **Processing:** Any operation performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- **Data Controller:** The entity that determines the purposes and means of processing personal data (in this case, The Emmanuel Ivorgba Center).
- **Data Processor:** An entity that processes personal data on behalf of the Data Controller (e.g., a third-party service provider).
- **Data Subject:** The identified or identifiable individual to whom personal data relates.

**V. Principles of Data Processing**

TEIC will adhere to the following core principles when processing personal data:

1. **Lawfulness, Fairness, and Transparency:** Personal data will be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. **Purpose Limitation:** Personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimization:** Personal data collected will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:** Personal data will be accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that inaccurate personal data are erased or rectified without delay.
5. **Storage Limitation:** Personal data will be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and Confidentiality:** Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

**VI. Collection and Use of Personal Data**

1. **Purpose Specification:** TEIC will clearly inform data subjects about the purposes for which their personal data is being collected at the point of collection.

2. **Consent:** Where consent is the legal basis for processing, TEIC will obtain explicit, informed consent from the data subject. Consent can be withdrawn at any time.
3. **Data Minimization:** TEIC will only collect the minimum amount of personal data necessary for the stated purpose.
4. **Legitimate Interests:** TEIC may process personal data based on legitimate interests, provided these interests are not overridden by the interests or fundamental rights and freedoms of the data subject. In such cases, data subjects will be informed of the processing.
5. **Sensitive Personal Data:** The collection and processing of sensitive personal data will be undertaken with explicit consent and will be subject to enhanced security measures and strict necessity.

**VII. Storage, Security, and Access**

1. **Secure Storage:** Personal data will be stored securely, whether in electronic or physical formats.
    - **Electronic Data:** Stored on secure, password-protected servers, encrypted databases, or approved cloud storage solutions with appropriate access controls. Regular data backups will be performed and stored securely.
    - **Physical Data:** Stored in locked cabinets or secure rooms, accessible only to authorized personnel.
2. **Access Controls:** Access to personal data will be granted on a "need-to-know" basis, limited to those staff or volunteers whose roles require such access.
3. **Security Measures:** TEIC will implement appropriate technical and organizational measures to protect personal data, including:
    - Firewalls and intrusion detection systems.
    - Regular software updates and patching.
    - Secure authentication methods (e.g., strong passwords, multi-factor authentication).
    - Data encryption where appropriate.
    - Physical security of premises and equipment.
4. **Confidentiality Agreements:** All staff and volunteers who handle personal data will be required to sign confidentiality agreements as part of their onboarding process.

**VIII. Data Sharing and Disclosure**

1. **Third-Party Service Providers:** TEIC may engage third-party service providers (data processors) to assist with its operations (e.g., for donor management, payroll, IT services). Where personal data is shared with such providers, TEIC will ensure that:
    - A written contract is in place that obligates the processor to protect the data and process it only according to TEIC's instructions.
    - The processor has implemented appropriate security measures.

2. **Legal Requirements:** TEIC may disclose personal data if required to do so by law or in response to valid requests from public authorities.
3. **Consent for Other Disclosures:** Personal data will not be shared with other third parties for their own marketing or other purposes without the explicit consent of the data subject.

**IX. Data Subject Rights**

Data subjects have certain rights regarding their personal data, including:

- **Right to Access:** The right to request access to their personal data that TEIC holds.
- **Right to Rectification:** The right to request correction of inaccurate personal data.
- **Right to Erasure (Right to be Forgotten):** The right to request the deletion of their personal data under certain circumstances.
- **Right to Restrict Processing:** The right to request the limitation of processing of their personal data.
- **Right to Data Portability:** The right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit it to another controller.
- **Right to Object:** The right to object to the processing of their personal data under certain circumstances.
- **Right to Withdraw Consent:** The right to withdraw consent for data processing at any time.

EIC will respond to all valid data subject requests within the timeframes required by applicable laws. Requests should be submitted in writing to the designated contact person.

**X. Data Retention and Disposal**

1. **Retention Schedule:** TEIC will maintain a data retention schedule that specifies how long different types of personal data will be retained, based on legal requirements, operational needs, and program purposes.
2. **Secure Disposal:** Once personal data is no longer required, it will be securely disposed of, whether through shredding of physical documents or secure deletion of electronic files, to prevent unauthorized access.

**XI. Data Breach Response**

1. **Incident Response Plan:** TEIC will have a plan in place to respond to data breaches.
2. **Notification:** In the event of a data breach that is likely to result in a risk to the rights and freedoms of individuals, TEIC will notify the relevant supervisory authorities and, where appropriate, the affected data subjects, in accordance with legal requirements.
3. **Investigation:** All suspected data breaches will be investigated thoroughly.

**XII. Training and Awareness**

All TEIC staff and volunteers will receive training on this Data Privacy and Confidentiality Policy upon onboarding and periodically thereafter. This training will cover the importance of data privacy, TEIC's responsibilities, and individual obligations.

**XIII. Roles and Responsibilities**

- **Board of Trustees:** Oversees the implementation and effectiveness of this policy.
- **Executive Director:** Is ultimately responsible for ensuring EIC's compliance with this policy.
- **Data Protection Officer (or designated individual/team):** Responsible for developing, implementing, and monitoring the policy; providing advice and training; and managing data subject requests and data breaches. (If TEIC does not have a formal DPO, assign these responsibilities to a senior staff member, e.g., Operations Manager, IT Manager).
- **All Staff and Volunteers:** Are responsible for understanding and adhering to this policy in their daily work and for reporting any potential breaches or concerns.

**XIV. Policy Review and Revision**

This Data Privacy and Confidentiality Policy will be reviewed at least annually, or more frequently as needed due to changes in legislation, technology, or TEIC's operations.

**XV. Approval and Effective Date**

Approved by the Board of Directors of The Emmanuel Ivorgba Center on: January 5, 2025

This policy is effective as of: January 5, 2025