DATA PROTECTION AND MANAGEMENT POLICY

JIREH DOO FOUNDATION POLICY DOCUMENT

JIREH DOO FOUNDATION (JDF)

MAY, 2020

TABLE OF CONTENT

SECTION ONE: DATA PROTECTION AND MANAGEMENT POLICY

BRIEF ORGANIZATIONAL PROFILE OF JIREH DOO FOUNDATION

Jireh Doo Foundation was founded in 2003 and became operational in the same year, JDF's uniqueness lies in her interventions for poor and excluded communities including services to single women and their children, orphans and vulnerable children with special considerations for those orphaned by HIV, Persons Living with HIV, Youth as well as advocating for favorable policies for these target group. Our interest also lies in providing relief assistance to those made vulnerable by human and natural disaster (IDPs). We make particular effort to nurture partnerships with public institutions, non-governmental organizations and agencies towards improving the lives of women, children, young people and other marginalized populations through participation, service delivery, fund raising, capacity building and networking amongst others in the achievement of sustainable development.

MOTTO

''Voice for the voiceless''

VISION

Jireh Doo Foundation envisions a better life for the underprivileged in our society.

MISSION STATEMENT

Jireh Doo Foundation is committed to improving the lives of the underprivileged through quality service delivery, resource mobilization, capacity development for relevant stakeholders and inclusive partnerships.

The need for an integrated and coherent translation of public policy response to action on current emerging developmental challenges especially as it affects our target audience gives rise to an integrated operational system, identity and structure for Jireh Doo Foundation. JDF is locally registered in Nigeria as a non-for-profit, National Non-Governmental Organization.

Core Values

Jireh Doo Foundation upholds the following values

- Respect for human rights
- Ensuring integrity in our relationship with stakeholders
- Make transparency and accountability a priority in all our actions.
- Encourage team work

- Effectiveness, Efficiency and Excellence
- Value for Money

AIMS AND OBJECTIVES

a. Strengthen capacity of stakeholders to respond to socio economic challenges of people and to ensure equity in the access and utilization of community resources and respect for human rights. Through this, JDF envisions a better life for the underprivileged in our society

b. Promote good governance and accountability at state and local levels through community mobilization, creative campaigning, and citizen participation.

c. Empowering capacities of community structures to engage and demand for accountability at all levels

d. Improve livelihoods of marginalized groups and their communities through empowerment and inclusive solidarity.

e. To respond to the needs of the distressed in our society

f. To ensure gender equity in the access and utilization of community resources and the respect for human rights

g. Develop a sustainable and credible referral systems that ensures the social wellbeing of target beneficiaries

h. To provide a purposeful and transparent leadership in the management and administration of the resources of Jireh Doo Foundation towards achieving her desired goal.

i. Build and retain a workforce that is bold, responsive and innovative capable of delivering high quality services to our target beneficiaries

THEMATIC FOCUS AND PROGRAM AREAS

In a world where development is a process, a condition and a reality, these areas of concern are of a key institutional and programmatic relevance to the vision and mission of Jireh Doo Foundation. Jireh Doo Foundation works in 5 broad program areas;

1. Humanitarian Response

- Food Security and Livelihood Advocacy
- Water Sanitation and Hygiene
- Emergency Response

- Gender Based Violence
- Disaster Management
- Child Case Management
- Livelihood Support
- Protection

2. Knowledge and Information Management

- Project Monitoring and Evaluation
- Analyzing and publicizing
- Operational Research
- Capacity Building
- Publications

3. Good Governance and Policy

- Advocacy for robust policy regulations
- Legislative monitoring and Advocacy
- Budget Tracking and Monitoring
- Civic Education
- Capacity building for policy makers at all levels

4. Gender, Women and Single Parents

- Single parents support and their children
- Advocacy
- Gender equity
- Capacity building
- Care and support
- Fundraising and empowerment

5. Child Development and Adolescent Empowerment

- Care and support
- Advocacy
- Child Case Management
- Child Education and Empowerment

- Capacity building

6. HIV and Health

- HIV and other disease Prevention
- Home Based Care and Support services
- Referral Services
- Mobile HIV Counseling and Testing services
- Community HIV and Health Education

1.0 BACKGROUND

Protecting individuals' Personal Data is an integral part of protecting their life, integrity and dignity. This is why Personal Data protection is of fundamental importance to Jireh Doo Foundation (JDF).

JDF as a humanitarian organization respects data protection principles, rules, laws and guidelines applied in data day-to- day data collection from different persons of concern, policy builds on existing guidelines, working procedures and practices that have been established in Humanitarian action and response in the most volatile environments and for the benefit of the most vulnerable victims of armed conflicts, other situations of violence, natural disasters, pandemics and other Humanitarian emergencies Some of these guidelines, procedures and practices pre-date the advent and development of data protection laws, but they all are based on the principles of human dignity and the same concept of protection which underpin data protection law. These guidelines have been set out, notably, in the Professional Standards for Protection of data.

1.1 INTRODUCTION

Individuals' Personal Data should be protected in all ways at all times and in any form. This is why Personal Data protection is highly emphasized by JDF. The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but Jireh Doo Foundation (JDF) as a Non-Governmental Organization (NGO) must respect their right to have control over their personal data and ensure it acts in full compliance with regulatory requirements at all times. If individuals feel that they can trust the organization with their personal data, this will also help to fulfill its aims and objectives.

1.2 PURPOSE OF THE POLICY

This Policy lays down the rules and principles relating to the handling of personal data of persons of concern to JDF**.** This Policy applies to all personal data that the organization processes regardless of the format or media on which the data are stored or who it relates to.

Its purpose is to ensure that JDF processes personal data in a way that is consistent with the international humanitarian guidelines and rules on Personal Data protection and other international instruments concerning the protection of personal data and individuals' privacy. The Policy will be complemented by Operational Guidelines that will provide guidance on its implementation, supervision and accountability.

1.3 SCOPE OF THE POLICY

This Policy applies to all members of staff employed by JDF, volunteers or interns, Vendors and consultants who offer services to the organization in various areas, as well as to data held by JDF in relation to persons of concern to the organization .The Policy continues to apply even after persons are no longer of concern to JDF.

You have a crucial role to play in ensuring that the Organization maintains the trust and confidence of the individuals about whom its processes personal data (including its own staff), complying with the legal obligations and protecting the organization's reputation. This Policy therefore sets out what the organization expects from you in this regard. Compliance with this Policy is mandatory for all JDF personnel; any breach of this Policy and any related policies and procedures may result in disciplinary action.

SECTION TWO: DATA PROTECTION AND MANAGEMENT PRINCIPLES

2.0 INTRODUCTION

The General Data Protection Regulation (GDPR) is based on a set of core principles that the organization must observe and comply with at all times from the moment that personal data are collected until the moment that personal data are archived, deleted or destroyed.

JDF must ensure that all personal data are:

1. Processed lawfully, fairly and in a transparent manner (**Lawfulness, fairness and transparency**)
2. Collected only for specified, explicit and legitimate purposes (**Purpose limitation**)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed or used (**Data minimization**)
4. Accurate and where necessary kept up to date (**Accuracy**)
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is or used (**Storage limitation**)
6. Processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage (**Security, integrity and confidentiality**)
7. Accountability and Supervision
8. Data is not shared or utilized for external or personal affairs without due approvals received from the National coordinator or her designee
9. Respect for human dignity when collecting data from beneficiaries

2.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

In order to collect and process personal data for any specific purpose, JDF must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, used or otherwise processed by the organization.

Processing personal data will only be lawful where at least one of the following lawful bases applies:

1. The data subject has given their **consent** for one or more specific purposes
2. The processing is necessary for the **performance of a contract** to which the data subject is a party (for instance a contract of employment or registration with the organization)
3. To comply with the JDF's **legal obligations**
4. To protect the **vital interests** of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)

JDF must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes for which data is collected.

JDF must ensure transparency runs throughout personal data collection and processing, the organization must ensure that any information provided by it to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. Where the organization has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the process into question.

2.2 PURPOSE LIMITATION

JDF must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal data have been collected.

The organization must ensure that it does not process any personal data obtained for one or more specific Purposes for a new purpose that is not compatible with the original purpose. Where the organization intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

2.3 DATA MINIMISATION

The personal data that JDF as an organization collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

JDF must only process personal data when necessary for the performance of her duties and tasks and not for any other purposes. Accessing personal data that the organization is not authorized to access, or has no reason to access, may result in disciplinary action and in certain circumstances, may constitute a breach of the rules and guidelines of personal data protection.

The organization may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

You must ensure that when personal data are no longer needed for the specific purposes for which they were collected, such personal data are deleted and destroyed.

2.4 ACCURACY AND DATA QUALITY

JDF shall ensure Personal Data is accurate and up to date as possible. Every reasonable step will be taken to ensure that inaccurate Personal Data are deleted or corrected without undue delay, taking into account the purposes for which they are processed. As a humanitarian Organization, we shall systematically review the information collected in order to confirm that it is reliable, accurate and up to date, in line with operational guidelines and procedures. In providing guidance on the frequency of review, account should be taken of (i) logistical and security constraints, (ii) the purposes of Processing, and (iii) the potential consequences of data being inaccurate. All reasonable steps should be taken to minimize the possibility of making a decision that could be detrimental to an individual or any person of concern.

The personal data that JDF collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when the organization discovers, or is notified, that the data are inaccurate.

The organization must ensure the update of all relevant records if there is awareness that any personal data are inaccurate. Where appropriate, any inaccurate or out-of-date records will be deleted or destroyed.

2.5 STORAGE LIMITATION

The personal data that JDF collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

The organization will maintain policies and procedures to ensure that personal data are deleted and destroyed after a reasonable period of time following expiry of the purposes for which they were collected.

JDF will regularly review any personal data processed by her in the performance of her duties and tasks to assess whether the purposes for which the data were collected have expired. Where appropriate, all reasonable steps must be taken to delete or destroy any personal data that the organization no longer requires in accordance with the Records Management Policies.

All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

2.6 SECURITY, INTEGRITY AND CONFIDENTIALITY

The personal data that JDF collects and processes must be secured by appropriate technical and organizational measures against accidental loss, destruction or damage, and against unauthorized or unlawful processing.

The organization will develop, implement and maintain appropriate technical and organizational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed
- likelihood and severity of the risks of such processing for the rights of data subjects

The organization will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective and it will be responsible for ensuring the security of the personal data processed by her in the performance of various duties and tasks. JDF must ensure that all procedures are followed in order to maintain the security of personal data from collection to destruction.

The organization will ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

- **Confidentiality:** means that only people who need to know and are authorized to process any personal data can access or handle it.
- **Integrity:** means that personal data must be accurate and suitable for the intended purposes
- **Availability:** means that those who need to access the personal data for authorized purposes are able to do so at any time.

There shall be no attempt to circumvent any administrative, physical or technical measures the organization has implemented as doing so may result in disciplinary action and in certain circumstances, may lead to a punishable crime.

The organization shall put in place appropriate procedures to deal with any personal data breach and will notify data subjects or the person of concern where and when it is legally required to do so.

If any party suspects that a personal data breach has occurred, he or she must contact the unit in charge of handling data or the personnel concern, immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach if necessary and this must be in compliance with the organization's personal data breach procedure.

2.7 ACCOUNTABILITY AND SUPERVISION

In order to ensure accountability for the protection of personal data in line with this Policy, JDF will set up an accountability and supervision structure.

2.8 SHARING PERSONAL DATA

Data sharing in humanitarian emergencies and response routinely require Humanitarian Organizations to share Personal Data with people handling the data and third Parties, including those based in other countries, or with International Organizations. Data protection laws restrict the sharing of and access to Personal Data with third Parties, in particular in case of transfers across borders or jurisdictions. Also, many data protection laws restrict International Data Sharing, which means any act of making Personal Data accessible outside the country in which they were originally collected or processed, as well as to a different entity within the same Humanitarian Organization, or to a Third Party, via electronic means, the internet, or others means.

Data sharing requires due regard to all the various conditions set out in the rules, principles and guidelines for data protection. Since data sharing is a form of Processing, there must be a legal basis for it and it can only take place for the specific purpose for which the data where initially collected and further processed. In addition, Data Subjects have rights in relation to data sharing and must be given information about it.

JDF will not share personal data with third parties unless the person concerned has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, the organization has

undertaken appropriate and due diligence of such processor and entered into an agreement with the processor that complies with the rules and guiding processes of data protection.

The transfer of any personal data to an unauthorized third party would constitute a breach of the Lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach.

SECTION THREE : RIGHTS OF PERSONS OF CONCERN AS DATA SUBJECTS

3. 0 INRODUCTION

The respect of Data Subjects' rights is a key element of data protection. However, the exercise of these rights is subject to conditions and may be limited in some situations.

An individual should be able to exercise these rights using the internal procedures of the Organization, such as by lodging an inquiry or complaint with the organization using the right channel. However, depending on the applicable law. The individual may also have the right to bring a claim in court or with a data protection authority.

3.1 THE RIGHT TO INFORMATION

Information in line with the principle of transparency, some information regarding the Processing of Personal Data should be provided to Data Subjects. As a rule, information should be provided before Personal Data are processed, although this principle may be limited when it is necessary to provide emergency aid to individuals.

Data Subjects should receive information orally and/or in writing. This should be done as transparently as circumstances allow and, if possible, directly to the individuals concerned. If this is not possible, the Organization should consider providing information by other means, for example, making it available online, or on flyers or posters displayed in a place and form that can easily be accessed (public spaces, places of worship and/or the organizations' offices), radio communication, or discussion with representatives of the community. Data Subjects should be kept informed, in so far as practicable, of the Processing of their Personal Data in relation to the action taken on their behalf, and of the ensuing results.

The types of information to be provided to Data Subjects may vary depending on the particular circumstances. A priority in this respect is that the information provided must be sufficient to enable them to exercise their data protection rights effectively.

When collecting personal data from a data subject, JDF should inform the data subject of the following,

In writing or orally, and in a manner and language that is understandable to the data subject:

1. The specific purpose(s) for which the personal data or categories of personal data will be processed
2. The importance of the data subject providing accurate and complete information
3. Whether such data will be transferred to Implementing Partner(s) or third parties or, where the data is being collected by an Implementing Partner on behalf of JDF, that the data subject is informed of this fact
4. The data subject's duty to keep JDF, and/or, as appropriate, Implementing Partners, informed of changes to their personal situation
5. Any consequences for refusing or failing to provide the requested personal data
6. The data subject's right to request access to their personal data, or correction or deletion of it
7. The data subject's right to object to the collection of personal data
8. The fact that if he/she has given Consent, he/she can withdraw it at any time
9. The period for which the Personal Data will be kept or at least the criteria to determine it and any steps taken to ensure that records are accurate and kept up to date
10. How to lodge a complaint with the Unit or personnel in charge of handling personal data

3.2 THE RIGHT TO ACCESS PERSONAL DATA

A Data Subject should be able to make an access request orally or in writing to JDF. Data Subjects should be given an opportunity to verify their Personal Data and should be provided with access. The exercise of this right may be restricted if necessary, for the protection of the rights and freedoms of others, or if necessary, for the documentation of alleged violations of international humanitarian laws or human rights law.

With due consideration for the prevailing situation and its security constraints, Data Subjects should be given the opportunity to obtain confirmation from JDF, at reasonable intervals and free of charge, whether their Personal Data are being processed or not. Where such Personal Data are being processed, Data Subjects should be able to obtain access to them, except as otherwise provided below.

The Organization's staff saddled with the responsibility of handling personal data should not reveal any information relating to Data Subjects or any person of concern, unless they are provided with proof of identity satisfying them that the Data Subjects are who they say they are.

JDF may not grant access to documents or personal data when overriding interests require that access not be given. Thus, compliance by the Organization with a Data Subject's access request may be restricted as

a result of the overriding public interests or interests of others. This is particularly the case where access cannot be provided without revealing the Personal Data of others, unless the document or information can be meaningfully redacted to blank out any reference to such other Data Subjects or such other Data Subjects have consented to the disclosure, without disproportionate effort. This is always the case when access would jeopardize the ability of the Organization to pursue the objectives of its Humanitarian Action or when it creates risks for the security of its staff or other persons of concern. This may also be the case for internal documents of the Organization, disclosure of which may have an adverse effect on Humanitarian action and response.

3.3 THE RIGHT TO REQUEST CORRECTION AND DELETION OF PERSONAL DATA

The Data Subject should also be able to ensure that JDF corrects any inaccurate Personal Data relating to him/her. Having regard to the purposes for which data were processed, the Data Subject should be able to correct incomplete Personal Data, for instance by providing supplementary information.

When this involves simply correcting factual data (e.g. requesting the correction of the spelling of a name, change of address or telephone number), proof of inaccuracy may not be crucial. If, however, such requests are linked to the Organization's findings or records (such as the Data Subject's legal identity, or the correct place of residence for the delivery of legal documents, or more sensitive information about the humanitarian status of the Data Subject), the organization may need to demand proof of the alleged inaccuracy and assess the credibility of the assertion. Such demands should not place an unreasonable burden of proof on the Data Subject and thereby preclude Data Subjects from having their data corrected. In addition, the Organization should require proof of identify that satisfies them that the Data Subjects are who they say they are before carrying out any correction.

A Data Subject should be able to have his/her own Personal Data erased from the Organization's databases where:

1. The data are no longer necessary in relation to the purposes for which they were collected or otherwise processed and/or further processed
2. The Data Subject has withdrawn his/her Consent for Processing, and there is no other basis for the Processing of the data
3. The Data Subject successfully objects to the Processing of Personal Data concerning him/her

4. The Processing does not comply with the applicable data protection and privacy laws, regulations and policies.

The exercise of this right may be restricted if necessary for the protection of the Data Subject or the rights and freedoms of others, for the documentation of alleged violations of international humanitarian laws or human rights law, or for legitimate historical , subject to appropriate safeguards and taking into account the risks for and the interests of the Data Subject. This can include the interest in maintaining archives that represent the common heritage of humanity.

3.4 THE RIGHT TO OBJECTION OF PERSONAL DATA PROCESSING

A data subject may object to the processing of his or her personal data where there are legitimate grounds related to his or her specific personal situation, at any time, to the Processing of Personal Data concerning them. If the objection is justified, JDF will no longer process the personal data concerned.

3.5 RESTRICTIONS OF THE RIGHTS OF DATA SUBJECTS

The right to ask the organization to restrict processing if:

- The data subject believes the personal data are inaccurate;
- The processing was unlawful and the data subject prefers restriction of processing over erasure;
- The personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim;
- The data subject has objected to the processing pending confirmation of whether the organization's legitimate interest for processing override those of the data subject.

JDF may refuse to provide a response or limit or restrict its response to a request or objection whereas:
It would constitute a necessary and proportionate measure to safeguard or ensure one or more of the following;

1. The safety and security of JDF, its personnel or the personnel of Implementing Partners; or
2. The overriding operational needs and priorities of JDF in pursuing its mandate
3. There are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing.

3.6 MODALITIES OF REQUESTS

Requests for information about access to, correction or deletion of personal data or an objection, may be made by the data subject or his or her authorized legal representative, or any other legal guardian. Requests are to be submitted orally or in writing to JDFs office where the data is being processed.

Before complying with any request or objection, the organization should satisfy itself of the identity of the person making the request or objection. The individual is required to identify him or herself in an appropriate manner. In the case of a legal representative or legal guardian, proof of such legal authority needs to be supplied. Requests and objections from parents or guardians of beneficiaries who are children should be evaluated against the best interests of the child.

SECTION FOUR: DATA SECURITY

4.1 CONTEXT

In a context of increasing collection of personal data, the use of multiple ICT assets including portable equipment, storage in a range of electronic data bases, transfers through various means and tools to a growing number of partners and other third parties and, in particular, the threats by a variety of adversaries, including criminal organizations, so-called hacktivists, state agencies and non-state actors with an interest in accessing confidential information about Persons of concern to JDF, the importance and challenge of data security cannot be underestimated.

The Data Protection Policy acknowledges these challenges and, bearing in mind the particularly vulnerable position of Persons of concern to JDF and the generally sensitive nature of their personal data, demands careful handling, a high level of data security, and the implementation of appropriate organizational and technical measures. In addition, the Policy takes into account the availability and quality of necessary equipment, the cost and the operational feasibility.

The Policy underlines the responsibility of the data controller who should ensure the implementation of organizational and security measures. Irrespective of organizational measures typically falling under the purview of the data controller, data security is a responsibility of all JDF personnel.

4.2 ORGANIZATIONAL MEASURES

Data controllers, assisted by their data protection focal points and other relevant staff, are encouraged to:

1. At country level, ensure that relevant data security measures are covered in Standard Operating Procedures

2. Ensure that trainings in data protection are organized or attended, including for Implementing partners
3. Raise the awareness for the responsible use of JDFs ICT assets and resources including email, internet, portable devices and equipment
4. Implement methods of safe transfer for personal data of Persons of concern
5. Routinely review and upgrade data security measures, e.g. through random monitoring and inspections and testing, assessing and evaluating the effectiveness of existing measures.

4.3 TECHNICAL MEASURES

Under technical measures, the Data Protection Policy mentions the maintenance of physical security of premises, portable equipment, individual case files and records, and ICT security through a number of control measures. This section elaborates on physical and electronic file management and distinguishes storage, access and user control that apply to both forms of file management. Data controllers may delegate the implementation of technical measures to their data protection focal points together with, other personnel responsible for handling of personal data.

4.3.1 Physical file management

Storage control. Responsible personnel are advised to observe the following:

1. Case files are kept in a lockable storage room or location designated for this purpose within JDF's premises, safe from water, fire and temperature damage
2. Access to the storage room to be controlled, monitored or restricted, for example, through access cards, physical control barriers, local or remote monitoring systems, with only authorized personnel granted access to them
3. The storage location needs to be kept locked when unattended. Copies of the key(s)/access cards are normally kept only by the Filing/Registration staff and the Representative and/or senior protection staff;
4. Outside the storage room, case files should be kept in a locked cabinet or drawer when personnel dealing with it is not at his/her desk or out of office, even for short breaks
5. Files should not be kept in interviewing rooms unless personnel are present;
6. Access to JDF premises shall be regulated, visitors logged in and out, and monitored properly by JDF staff while within the office

Access control to physical files (within and outside the designated storage location):

1. Case workers should have access to physical files of cases that have been assigned to them, in line with their duties and responsibilities
2. Reviewing officers should have access to files they are responsible for reviewing and for quality checks, in line with their duties and responsibilities
3. Non-protection personnel may only request access to case files through the Senior Protection Officer (or equivalent) within the organization
4. Interpreters should normally not have access to individual case files. Where they exceptionally have been assigned tasks related to case processing, as approved by the data controller, access to individual files needs to be strictly limited to necessary documents related to authorized responsibilities, and should be closely supervised.

User control. Tracking and recording the movement of physical files:

1. A file check-out/check-in procedure shall be in place, with an up-to-date record of who has, and have in the past had, access to individual case files
2. The personnel in charge of personal data should register the file number, date, and initials/name of the personnel requesting the file onto the file movement log upon release, and note its date of return and initials/name of the personnel who returned it
3. Requests, releases, transfers and returns of files should normally be recorded on a File Action Sheet. File movement logs should be sought stored electronically wherever possible
4. JDF personnel shall not remove individual case files from the premises. Except when authorized by the data controller or Senior Protection Officer based on a written request.
5. There shall be a limit to the number of files an individual caseworker can have in his/her possession at any given time (normally a maximum of 20).

General advice on case files management:

1. Create, assemble and verify Individual case files at the time of registration
2. Clearly mark files on the outside with the file number (or unique identification)
3. In principle, one file for one Person of concern in one office for use by all functional units
4. Insert action sheet, including of all actions and dates related to the case (scheduled interviews, referrals, house visit, added or removed documents etc.) and keep up-to-date
5. Keep documents in chronological order (newest documents placed on top)

6. Non-digitized photographs recommended subject to tamper-proofing measures (such as dry or wet seal stamps), with the name and registration number of the Person of concern on the back
7. Keep only copies of original documents provided by a Person of concern and hand back original. The copy should be noted "copy" and "original seen"
8. Internal notes to be dated and signed, with the name and title of the caseworker
9. Consider keeping strictly confidential information

4.3.2 Electronic file management

Personal data stored in electronic format is particularly vulnerable to accidental, unlawful or illegitimate destruction, loss, alteration, as well as unauthorized disclosure, due to the ease with which it can be copied, transferred, and even posted on the Internet. Access to such data should therefore be carefully restricted, managed and monitored. Data controllers, with close support from data protection personnel, are responsible for ensuring that databases and supporting IT infrastructure are established and used according to standards, JDF shall ensure the following measures;

Storage control

1. JDF data Operations shall use corporate or recommended humanitarian organizations tools, document management applications, and network drives with controlled accessibility. The use of non-approved tools can undermine data security
2. Server locations shall be physically secure, with adequate electrical, water and fire safety. IT Officers or personnel of equivalent positions are responsible for adequate back-up procedures
3. JDF has reliable access to the internet and so shall store personal data electronically where necessary. Personal data of Persons of concern shall not be stored on personal network drives

Access control to electronic files

1. Access to electronic files shall be tiered, so that personnel only have access to what they need to for the purposes of performing their duties and responsibilities
2. Operations are recommended to establish procedures for the submission and review of user access requests to ensure that users are only given access to the data they need. Access rights are normally defined by the Heads of Units, approved by the data controller or personnel in charge.

3. A regular review of access rights shall be recommended, e.g. every 6 months, to ensure that personnel who no longer require access have their permissions revoked.

4.4 AUDIO AND VIDEO RECORDING OF COUNSELLING AND INTERVIEWS WITH PERSONS OF CONCERN

JDF shall ensure that operations which are audio or video recording when counselling or interviewing be stored securely preferably electronically with access restricted to authorized personnel only. Recording devices will be kept in a secure location, and all electronic copies of videos/tapes clearly linked to a physical file, and securely disposed of when their retention periods have elapsed or are no longer needed. Operations which are considering introducing cameras in interview rooms and/or video recording for interviews with persons of concern are recommended to consult data protection personnel, in order to reach the best decision based on security, data protection and case management considerations.

4.5 DATA SECURITY PROCEDURES AND PRACTICES

Data security is about technology, ICT assets and resources, but even more about their use. Research repeatedly shows that human error is the leading cause of data and security breaches. Weak data security practices by personnel (the human factor) can undermine an organization's efforts to protect personal data and JDF is not an exception. All personnel with access to JDF's ICT assets and resources (including basic tools such as computers and emails) are therefore advised to familiarize themselves with existing data security procedures and practices, and to avoid behaviors which may pose risks to the personal data of Persons of concern and JDF´s operations more broadly. A short summary of these procedures and practices includes:

4.5.1 Secure use of ICT assets and resources (including email and internet)

All JDF personnel are bound by internal policies on the use of electronic mail, the internet as well as the personal use of computers and other technology resources.

In terms of recommended practices, all JDF personnel are encouraged to:

1. Maintain a healthy distrust and defensive posture in respect to unknown persons and communications, for example by not clicking on links or opening attachments in emails that come from unknown addresses or seem suspicious, disclosing sensitive information about themselves or colleagues on insecure websites, or giving passwords to others
2. Pursue safe internet browsing practices. JDF personnel should not install video players or browser extensions on their Personal Computers without the advice of an IT personnel, as these may contain malware.
3. Computers that do not have up-to-date anti-virus, patches or firewalls are far more likely to be infected by malicious software and applications ('malware'). IT personnel should ensure that all office computers are using up-to-date software and operating systems and licensed anti-virus software, to download and install automatically
4. Report suspicious activity to the appropriate quarters to allow swift and effective measures. Potential breaches, such as compromised accounts or systems, lost or stolen computers, the unauthorized release of protected information, system downtime, and the detection of malicious software, should also be reported to the data controller.

4.5.2 Secure use of portable ICT equipment (including laptops, smartphones and USB drives)

Laptops, tablets, smartphones, and other portable devices have the advantage of being used outside JDF premises but may be lost or stolen, which may lead to loss of personal data and potential unauthorized access. Portable devices may also be more vulnerable to malware, and users are less likely to apply the latest security patches and have less secure operating systems. To limit the risks to persons of concern, all JDF personnel are recommended to:

1. Minimize the amount of personal data of persons of concern stored on their portable devices, including on smartphones and laptops
2. Ensure that all portable devices are password/PIN protected, respect guidance on the use of passwords, set to 'auto lock' when not in use and keep in possession or in safe locations at all times
3. Portable or removable devices (such as USB drives and memory cards) should in principle not be used to store or transfer personal data. If their use is unavoidable, the devices should be encrypted (seek advice from the IT personnel), kept physically secure, and the data erased immediately upon completion of the task

4. JDF personnel returning a device to the organization should ensure that they erase all their emails, messages and any other files which may contain personal data of Persons of concern (POCs)
5. Lost or stolen devices which have been used for personal data should be reported to the data controller and IT personnel, and any passwords changed immediately

4.5.3 Secure use of ICT assets during mission travel and remote working arrangements

Remote working arrangements and mission travel carries additional risks, as networks and resources may not be as secure. All JDF personnel should be aware of the following:

1. Public Wi-Fi networks and open access points (i.e. which do not require a password) pose the greatest risk, because users may be exposed to 'sniffing' (the capture of data sent across insecure networks) and 'man in the middle attacks' (using fake or malicious Wi-Fi 'hotspots'), and at greater risk from viruses, spyware, malware, and 'phishing' attempts. Personnel are therefore advised to avoid such networks. If used exceptionally, file sharing should be disabled, the wireless network settings changed to 'public' and personnel remain vigilant for suspicious activity.
2. Personnel working from home are encouraged to ensure that their wireless networks are secure. Access to networks should be controlled, WPA2 security protocol applied, and default router administrator passwords replaced. Seek advice from the IT personnel
3. Border guards in an increasing number of countries demand that individuals open their laptops, turn on mobile phones and enter or handover passwords to access data on such devices. In such a situation, JDF personnel are advised to comply with a request to turn on their electronic devices to allow a non-intrusive visual inspection (for the purposes of verifying that the devices function), but not to allow the opening, reading or downloading of documents. Requests for handing over of pin codes or passwords, or for examining the device without it being in the presence of the staff member should be declined. If necessary, staff members should request to see the guards' supervisor in order to make clear that the device(s) contain documents which are confidential and inviolable as part of JDF's archives.

4.6 SECURE COMMUNICATIONS AND DATA TRANSFERS

There is a high risk of data breaches when personal data is communicated or transferred, for instance from JDF to a third party. E-mails and SMS messages may be intercepted during transmission and/or retained by surveillance programs, thus putting persons of concern at risk of harm, in particular if

accessed by countries of origin. On this issue, the Data Protection Policy states that "in order to ensure and respect confidentiality, personal data must be transferred only through the use of protected means of communication.

In order to reduce the risk of personal data breaches during communication and transfer of personal data, JDF personnel are recommended to:

1. In principle, use only JDF and humanitarian organizations developed and approved tools to transfer personal data
2. Exercise caution regarding the use of third-party file-sharing tools (Approvals must be given)
3. It is impossible to guarantee the confidentiality of any electronic message transmitted outside the JDF system via the internet. No information of a confidential nature should be sent by e-mail via the internet. More secure alternatives include the use of JDF secure file transfer protocol (FTP) service, and encrypted portable media devices
4. Personal data should not be transferred using personal email accounts (e.g. Gmail, Yahoo or Hotmail), or through social media accounts (e.g. Facebook, Twitter)
5. If E-mail is used, ensure that additional measures are taken to protect the content, such as encrypting the email or its attachment. When sharing password protected files, the password should be sent via an alternative means of communication (such as phone call or text message)
6. SMS should be avoided as a means to communicate personal data, internally within JDF, externally and with persons of concern. Text messaging services that are encrypted end-to-end are more secure than SMS messages and should be used instead
7. Seek advice from the IT personnel on which tools to use for different purposes and in different operational scenarios

4.6.1 Communication with communities through "bulk SMS" and messaging applications

Bulk SMS and messaging applications present opportunities for enhanced communication with displaced communities, in particular areas which are difficult for JDF to access. JDF personnel should, however, be aware of the potential lack of security related to these tools, which may reveal the identity and location of individuals or communities to third parties, as well as collect personal data and metadata, and facilitate access for law enforcement agencies and other state authorities.

To minimize protection risks, JDF recommends the use of such tools only for purposes such as emergency or security broadcasts, administration of assistance distribution, and monitoring. They should, as far as possible, be avoided for protection sensitive information.

4.6.2 The use of electronic and digital survey tools

JDF shall ensure the use of survey tools and mobile devices to collect data from persons of concern which allows for more efficient assessments than paper-based systems. In light of the potential data protection challenges, personnel are strongly advised to consult the IT personnel to select survey tools and modalities which ensure that personal data is only collected, processed and retained in accordance with the requirements of the Policy.

4.7 DEFINITION OF TERMS

Aggregate data: Means data is combined in a way to show values or trends without including the records of individual data subjects or data that would render an individual data subject identifiable.

Assent: Is the expressed willingness and views of a child to participate in assistance or protection activities and services in situations where he/she cannot legally provide formal consent to the processing of personal data due to age, level of maturity and/or other factors.

Consent: Means any freely given and informed indication of an agreement by the data subject to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action

Data Sharing: Means any act of transferring or otherwise making personal data of persons of concern accessible within or between JDF offices, or to a JDF partner or third party.

Data subject: Means any individual falling within the scope of the Data Protection Policy whose personal data is subject to processing by JDF.

Data Transfer Agreement: Is an agreement between JDF and a third party which states the terms and conditions of the use of personal data, including the specific data sets to be shared, the mode of data transfer, for what purposes the data may be used, data security measures, and related issues.

Data Controller: Means the JDF staff member, usually the Representative of the organization, who has the authority and accountability for overseeing the management of, and to determine the purposes for, the processing of personal data.

Data minimization: Means a standard procedure to minimize data protection risks and ensure that the data collected, shared or otherwise processed is necessary and relevant to achieve a specified purpose.

Data Processor: Means any JDF staff member or other natural person or organization, including an Implementing Partner or third party that carries out processing of personal data on behalf of the data controller.

Data Protection Focal Point: Means, in principle, the most senior JDF protection staff member in the organization, who has been designated by the data controller to assist in carrying out his or her responsibilities regarding this Policy.

Humanitarian Action: Means any activity undertaken on an impartial basis to carry out assistance, relief and protection operations in response to a Humanitarian Emergency. Humanitarian Action may include "humanitarian assistance", "humanitarian aid" and "protection".

Humanitarian Emergency: Means an event or series of events (in particular arising out of armed conflicts or natural disasters) that poses a critical threat to the health, safety, security or wellbeing of a community or other large group of people, usually over a wide area.

Humanitarian Organization: Means an organization that provides aid to alleviate human suffering, and/or protects life and health, and upholds human dignity during Humanitarian Emergencies in accordance with its mandate and/or mission

JDF personnel: Means all individuals working for JDF including staff members, affiliate workforce (Volunteers, interns, vendors).

Person of concern: Means a person whose protection and assistance needs are of interest to JDF. This includes refugees, asylum-seekers, stateless persons, internally displaced persons and returnees.

Processing : Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available to any party, alignment or combination, restriction, erasure or destruction.

Personal data: Means any data related to an individual who can be identified from that data; from that data and other information; or by means reasonably likely to be used related to that data. Personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, individual registration number, occupation, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs.

Subject access request: Means a request from a person of concern, or their legal representative, to obtain information from JDF about the personal data that it holds on them, and any associated requests to amend or delete such data. Subject access requests may also be received from family members in respect to data held in JDF's archives.

Third party: Means any natural or legal person other than the data subject, JDF or an Implementing Partner. Examples of third parties include national governments, international governmental and non-governmental organizations, private sector entities or individuals.

Statement of commitment of Jireh Doo Foundation Data Protection Policy

I,_____, have read and understand this Data protection policy (2020). I agree with the values and beliefs contained within it and agree to work in accordance with the standards guidelines and procedures it outlines while working **with Jireh Doo Foundation**

Name: _____

Job Title: _____

Signature: _____ Date: _____