1/1/2023

MANAGEMENT INFORMATION POLICY

FAROF

Freehearts Africa Reach Out Foundation

Saving Lives One @ a Time

FAROF 2023

Contents

1. INTRODUCTION

The Freehearts Africa Reach Out Foundation (FAROF) acknowledges that information technology should be at the service of every citizen. Information technology development shall take place in the context of international co-operation. Information technology shall not violate human identity, human rights, privacy, or individual or public liberties.

FAROF is committed to international compliance with data protection laws. This management information system policy applies worldwide to FAROF and is based on globally accepted, basic principles on data protection and information management. Ensuring data protection and information management is the foundation of trustworthy relationships and the reputation of FAROF as a credible organization.

The management information policy ensures the adequate level of data protection as prescribed by relevant legal frameworks. The FAROF management information policy is meant to be a practical and easy to understand document to which all FAROF departments, stakeholders and partners can refer to.

2. OBJECTIVES

By adopting such a policy, FAROF seeks to:

- Promote open access to data and information produced at FAROF in order to facilitate data and information discovery, sharing and collaboration;
- Clarify responsibilities so that researchers and research support staff understand what is required from them;
- Set out the organization's obligations including the provision of facilities for the management of data and training, support and guidance on good practice in data and information management;
- Improve access, discoverability, usability and visibility of the FAROF's research outputs, documents and knowledge products, innovations and technologies;
- Protect the legitimate interests of the FAROF and of other parties;
- Ensure that data and information are protected from unauthorized access and mitigate the risks associated with the theft, loss, misuse, damage or abuse.

3. SCOPE OF POLICY

This management information policy applies to all entities of FAROF.

- The policy applies to all FAROF staff and governance members.
- The provision of this policy may also be applied to any person employed by an entity that carries out missions for FAROF.
- In particular, this policy applies to implementing partners, suppliers, sub-grantees, stakeholders and other associated entities.

FAROF's management information system policy applies to all personal data that FAROF holds relating to identifiable individuals, meaning any information relating to an identified or identifiable individual.

4. FAROF'S SET OF DATA AND DEFINITIONS

FAROF management information system policy applies to all sets of personal data, currently stored, maintained and handled by FAROF and more specifically to the following identified sets of personal data:

- FAROF's personnel, including interns and volunteers,
- FAROF's direct and indirect beneficiaries, including interviewees,
- FAROF's individual donors and sympathizers,
- FAROF's contractors, suppliers, consultants, implementing partners currently under contract with FAROF.

Personal data herein referred to, means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This can include in particular:

- Names of individuals
- Postal or living addresses
- Email addresses
- Telephone numbers
- Identity card and passport
- Date and place of birth
- Identification of relatives
- Fingerprints
- Business reference
- Geo-referencing

Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

This also applies to all data and information products in any medium including:

- Reports
- Data and database, models and algorithms
- Audio, video and photographs
- Metadata, software, websites and its content and application.
- Standard operating procedure, guidelines, manuals and protocols.

Regarding research, the policy applies to all projects where FAROF is the lead institution. If the organization is not the leader, then the contractual agreement must specify the principles guiding the management of data and research outputs generated by the project. While the Data and Information Management Policy applies to all FAROF data and information, legal and contractual obligations limit the application of this Policy in some cases. Also, the Institute does not provide access to data and information of which the dissemination could compromise new findings, the security of staff and their families, partners and FAROF assets.

5. PRINCIPLES

- The following principles are set forth to govern the appropriate usage and management of data and information:
- Unless explicitly agreed the organization rather than any individual or unit, owns the data and information created by researchers and other staff during the term of their employment with the organization;
- The organization undertakes to provide appropriate resources, training, support and guidance to researchers and research support staff around data management;
- Data management is a shared responsibility within the organization and staff will work in partnership to satisfy the requirements of the Policy, establish a culture of sound data management practice, and realize the benefits of data sharing;
- All FAROF staff are responsible for making themselves familiar with and adhering to this Policy;
- If a staff leaves the organization, he or she must pass on the stewardship of any data created during their employment before their departure. In the

absence of an agreed successor for the data and information, the stewardship will devolve upwards to the Data Management Unit.

- Management and sharing of data should be supported through the allocation of funding;
- All projects must have from their inception a data and information management plan (DMP), which addresses the arrangements for data management throughout the project life-cycle and for the long term preservation;
- The ownership, use and sharing of data and outputs produced by/and with FAROF should be referred to in all relevant documents and procedures;
- Data and information will be managed as a corporate resource to support decision making, the delivery of programs and projects, the administration of the organization and to improve partnership and collaboration and the quality of services to all stakeholders;
- Data and information will be stored, documented, archived and made accessible for the long term in accordance with contractual, funding and legal requirements;
- Data and information will be managed according to defined needs and according to data management principles, standards, procedures, guidelines;
- All data and information must be accompanied with the metadata;
- FAROF will comply with legal and regulatory requirements relating to research data management, such as those relating to ethics, data protection in line with the Research Ethics Policy and the Code of Conduct to support FAROF integrity.

5.1. PRINCIPLES FOR PROCESSING PERSONAL DATA

Fairness and Lawfulness

- When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.
- Collected data shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing.
- Individual data can be processed upon voluntary consent of the person concerned.

Restriction to a specific purpose

- Personal data can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible
- with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification.
- However, further data processing for statistical, scientific and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is not used to take decisions with respect to the data subjects.

Transparency

- The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be made aware of, or informed of: o The purpose of data processing; o Categories of third parties to whom the data might be transmitted
- Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: compliance with any legal obligation to which FAROF is subject; the protection of the data subject's life; the performance of a public service mission entrusted to FAROF.

Confidentiality and Data Security

- Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

Deletion

- Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

Factual Accuracy and Up-to-datedness of Data

- Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

5.2. DATA PROCESSING

Consent to Data Processing

- Individual data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. In certain exceptional circumstances, consent may be given verbally.

Data processing Pursuant to Legitimate Interest

- Personal data can also be processed if it is necessary to enforce a legitimate interest of FAROF. Legitimate interests are generally of a legal (such as filing, enforcing or defending against legal claims), audit or financial nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the individual merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of personal data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the organization in performing the control measure (e.g. compliance with legal provisions and internal rules of the organization) must be weighed against any interests meriting protection that the individual affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

Telecommunications and Internet

- Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by FAROF primarily for work-related assignments. They are a tool and an organizational resource. They can be used within the applicable legal regulations and internal FAROF communication policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

- There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by FAROF that block technically harmful content or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the internet and internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of policies and/or procedures of FAROF. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the FAROF regulations.

Rights of the Data Subject

All individuals who are the subject of personal data held by FAROF are entitled:

- To request information on which personal data relating to him/her has been stored, how the data was collected, and for what intended purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. If personal data is transmitted to third parties, individuals should be informed of such a possibility. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
- To request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
- To object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

5.3. TRANSMISSION OF PERSONAL DATA

Transmission of personal data to recipients outside or inside FAROF is subject to the authorization requirements for processing personal data under Section 6 and requires the consent of the data subject. The data recipient must be required to use the data only for the defined purposes. In the event that data is transmitted to a recipient outside FAROF, this recipient must agree to maintain a data protection level equivalent to this Policy. This does not apply if transmission is based on a legal obligation.

The processing of personal data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the individual that merit protection must be taken into consideration. In certain circumstances, the FAROF management information system Policy allows personal data to be disclosed, based on a legal obligation, to law enforcement agencies, without the consent of the data subject.

Only FAROF's Chief Executive Director can validate any such disclosure in writing, ahead of the disclosure, after ensuring the request is legitimate, motivated by the requester, appropriate, necessary and does not pose a threat or direct risk to FAROF.

Before approving such disclosure, FAROF's Chief Executive Director will check that the recipient of the data uses the data for the defined purposes only, and that it demonstrates the capacity and will to abide by such an obligation. Where necessary, FAROF's Chief Executive Director will refer to legal advisers for advice, and to FAROF Committee for validation, notably but not only in cases involving direct security threats and implications or global organizational risks including reputation.

5.4. CONFIDENTIALITY OF PROCESSING

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principle applies. Duly-authorized employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

5.5. PROCESSING SECURITY

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). The technical and organizational measures for protecting personal data are part of FAROF’s management and must be adjusted continuously to the technical developments and organizational changes.

5.6. VIOLATION, SANCTION AND REPORTING

Any failure to comply with the current policy or to deliberately violate the rules set in the policy will result in the launch of an appropriate investigation by FAROF.

Depending on the gravity of the suspicion or accusations, FAROF may suspend staff or relations with other stakeholder during the investigation. This will not be subject to challenge.

Depending on the outcome of the independent investigation, if it comes to light that anyone associated with FAROF has deliberately violated the rules set in the policy for its personal profit or any other usage of personal data, or has systematically and deliberately contravened with the principles and standards contained in this document, FAROF will take immediate disciplinary action and any other action which may be appropriate to the circumstances. This may mean, for example, for:

- Employees - disciplinary action/dismissal;
- Trustees, officers and interns - ending the relationship with the organization;
- Partners - withdrawal of funding/support;
- Contractors and consultants - termination of contract.

Depending on the nature, circumstances and location of the case and violation, FAROF will also consider involving authorities such as the police to ensure the protection of personal data and victims. The reporting of suspected or actual violations to this policy is a professional and legal obligation of all staff and partners. Failure to report information can lead to disciplinary action.

FAROF encourages its staff and stakeholders to report suspected cases which involve any FAROF staff, consultants, board members, guests or staff of FAROF's partner organizations, their board members, staff and or suppliers.

FAROF encourages its staff and stakeholders to report suspected cases through the following means:

- Staff and interns can report contacting
  standard lines of hierarchy (contained in staff Terms of Reference);
  the Head of Human Resources.
- Beneficiaries and their representatives can report using the Complaints and Response Mechanism (CRM) 1.
- Suppliers and contractors can use the confidential email address transparency.@farof.org
- Individual donors and sympathizers can refer to the confidential email address transparency.@farof.org.

All reports will be treated as confidential in line with FAROF Code of Conduct and FAROF's Human Resources guidelines.

FAROF will not tolerate false accusations which are designed to damage a member of staff's reputation. Anyone found making false accusations will be subject to investigation and disciplinary action.

6. ROLES AND RESPONSIBILITIES

All staff, interns, consultants and volunteers engaged by FAROF handling data and information are responsible for the management and security of the data and information they create, capture, store and use. They should familiarize themselves with this Policy However, the following roles and responsibilities are defined, for specific staff and groups, for the purpose of establishing clear governance and accountabilities over data and information.

Management

- Provide support and leadership to ensure that the objectives of the Policy can be delivered;
- Provide appropriate communication, training and advisory services to ensure that data and information are made available, subject to meeting appropriate requirements, in the location specified in the data management plan;
- Provide safe, secure and sustainable infrastructure and repositories to make data and information available, while respecting the rights of stakeholders in terms of confidentiality, intellectual property and data ownership;
- Encourage the use of existing technologies to maximize efficiencies and investments already made in existing technologies;
- Ensure that performance assessment includes data and information management

Researchers

- Include cost and time implications of data storage and management in grant proposals;
- Develop data management plan that addresses the creation, management, storage and publication of data and the production of descriptive metadata;
- Ensure the quality of data so that it is usable and fit for purpose;
- Ensure that research data are deposited and preserved in appropriate repository, unless specified otherwise in the data management plans;
- Plan for the custodial responsibilities for research data on departure from the organization;
- Consult with the Data Management Unit regarding good practice in research data management;

Database, Web and Platform Managers

- Implement, document and maintain processes, technologies, and procedures to comply with data integrity, security confidentiality and accessibility to meet institutional requirements;
- Provide data and information management services which result in the highest quality data in their specific subject area;
- Implement and maintain data and metadata quality requirements and rules for assigned data sets;
- Support staff training to ensure that data is captured and used accurately and appropriately;

- Provide input into data policies, standards and procedures;
- Champion the implementation of data management standards and processes.

Human Resources Unit

- Ensure that competencies, skills and attributes related to data and information management are included in relevant staff job description and performance assessment;
- Ensure that custodial responsibilities for data and information are included in the Handover Notes to ensure the continuity and the smooth transition and operations

7. Data Management Tools

This section outlines FAROF data collection and survey tools.

At FAROF we adopt the most reliable data collection tools and as approved by our Donor and the FAROF Management and Trustee Board. Some of the approved Data management Tools adopted by FAROF are:

7.1. Power BI-Data visualization (Microsoft 360 office)-

Microsoft Power BI is a data visualization and reporting platform that is used by businesses and professionals every day. While the platform is commonly used by business analysts, it is also designed to be easily accessible for those without any specialized data knowledge.

Microsoft Power BI is a data visualization platform used primarily for business intelligence purposes. Designed to be used by business professionals with varying levels of data knowledge, Power BI's dashboard is capable of reporting and visualizing data in a wide range of different styles, including graphs, maps, charts, scatter plots, and more. Power BI's "AI Insights" functionality, meanwhile, uses artificial intelligence to find insights within data sets for users..

Power BI itself is composed of several interrelated applications: Power BI Desktop, Pro, Premium, Mobile, Embedded, and Report Server. While some of these applications are free-to-use, paid subscriptions to the pro and premium versions provide greater analytics capabilities. Power BI is also a part of Microsoft's Power Platform, which includes Power Apps, Power Pages, Power Automate, and Power Virtual Agents. Created as "low-code tools," these applications help businesses analyze and visualize data, design business solutions, automate processes, and create no-code chatbots.

7.2. Survey monkey-

SurveyMonkey is online survey software that helps you to create and run professional online surveys. It is very powerful and a well known online application.

Why we Use Survey Monkey?

Surveys are important to collect feedback, opinions, criticism and suggestions from the general public and customers.

SurveyMonkey presents all the tools necessary for you to create strong, professional surveys easily.

Analysis happens in real time. Results are viewed as respondents complete their surveys. However, if you would like to download and keep a copy of the survey and the results, an upgrade to premium will be necessary. A premium account gives you access to multiple custom reports, response download, custom chart creation and download functionality, and options to share responses

7.3. National OVC Management Information System (NOMIS)

In 2011, the Federal Ministry of Women-Affairs & Social Development (FMWASD) FMWASD adopted the National OVC Management Information System (NOMIS) as the national electronic platform for the management of data for OVC programs in Nigeria.

This 2020 assessment reviewed the status of the National OVC Management Information System (NOMIS) system in Nigeria. It was conducted by the Data.FI project—funded by the U.S. Agency for International Development (USAID) and U.S. President’s Emergency Plan for AIDS Relief (PEPFAR)— and identified current system limitations, strengths to build upon, and improvements necessary for the system to be sustainable.

8. ANNEX

Glossary of terms

- ***Data*** is facts, figures or individual pieces of information that is captured through the operation of the Institute. In the scientific community, data is the recorded factual material commonly accepted as necessary to validate research results. Information is data that has been interpreted so that it has meaning for the user.
- ***Data management*** is the function that develops, manages and executes policies and processes that collect, protect, deliver, and enhance the value of data and information assets to meet the data availability, quality and security needs of the Institute.
- ***A data management plan (DMP)*** is a formal document that outlines how an activity or project will produce, collect, process, store and publish data both during the research/activity and after the research /activity is completed. In developing a data management plan, researchers should consider which data would be required to verify their results and which data would have the highest potential and value for reuse by others. The DMP forms the basis of data management throughout the project lifecycle.
- ***Data security*** refers to methods of protecting data from unauthorized access, modification, or destruction.
- ***Information*** refers to data that have been processed into a meaningful form.
- Institutional repository is a service for storing and providing online access to digital content.
- ***Metadata*** is structured data that describes and/or enables finding, managing, controlling, understanding or preserving data over time. Metadata includes, but is not restricted to, characteristics such as the content, context, structure, access, and availability of the data