WARRIOR SQUAD
Foundation
Together we can build Hope

Responsible Program Data Policy

Approved on 20th June 2018

Introduction

As a rights-based organization, WSF is committed to using data responsibly in order to uphold the rights of the individuals, groups and organizations with whom we work. Using data responsibly is not just an issue of technical security and encryption but also of safeguarding the rights of people to be counted and heard; ensure their dignity, respect and privacy; enable them to make informed decisions; and not be put at risk, when providing data.

WSF recognizes that people have rights with regards to the information related to them and that WSF has a responsibility to uphold those rights. The rights that form the backbone of this policy are:

1. **Right to be counted and heard**
2. **Right to dignity and respect**
3. **Right to make an informed decision**
4. **Right to privacy**
5. **Right to not be put at risk**

This policy should not be seen as restricting or discouraging; rather it sets out to facilitate the invaluable contribution that data makes to the quality of WSF's work, upholding accountability and allowing WSF to raise the voice of those with whom we work.

For the purposes of this policy, data are considered to be the physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means. Data may be numerical, descriptive, audio or visual. The formal term for individuals from whom data are collected is "data subjects". In this policy, however, we use the term "participants" and expand the definition to include any group, cooperative, or other entity with which WSF works that provide program data.

This document sets out the policy for the treatment of program data by WSF throughout the data lifecycle from planning to collection through to disposal. This data may pose varying degrees of risk to different stakeholders, including but not limited to the people who provide data, those that collect it, and WSF; therefore, this policy includes definitions & requirements for managing high-, medium-, and low-risk data.

This policy pertains to data from all of our programs: Humanitarian, Advocacy and Campaigns, and Long-Term Development (both project and program), funded by both restricted and unrestricted funds. It will apply to all aspects of the project and program cycle as well as research. WSF will uphold this policy for all projects where WSF is the data controller. WSF is responsible for ensuring that all external individuals or organizations it works with during the data lifecycle (partners, contractors, etc.) comply with the policy.

This policy is designed to be forward-looking and prepare WSF for the future, establishing systems to enable the organization to take full advantage of the current opportunities and future potential of the data revolution. Recognizing that the policy applies to a rapidly-changing technological context, WSF has a responsibility to stay abreast of the implications of these changes for its work. A set of minimum standards and guidelines accompanies this policy to provide details on how to operationalize the requirements and will be updated periodically.

Policy Elements

A. Right to be counted and heard

In order to ensure the rights of vulnerable and marginalized populations, including women, it is important that they are able to be counted and adequately represented as part of the information WSF collects and uses.

1. Where appropriate and possible, WSF will make every effort to ensure that vulnerable groups including women are fully represented in data collection, and that the resulting datasets can be disaggregated by gender and other relevant categories.
2. WSF will make all reasonable effort to ensure the inclusion of participants from marginalized populations.
3. WSF will ensure the accuracy of data collected, stored, and used, including making efforts to keep information up-to-date and relevant
4. WSF will appropriately analyse, utilize, and disseminate the information it collects in order to ensure participants' right to be heard, especially within marginalized populations. This dissemination should include communicating findings to the surveyed population as part of WSF's commitment to social accountability.

B. Right to dignity and respect

WSF will ensure that a participant's personal dignity is maintained and respected in all phases of the data lifecycle.

1. Data will be collected in a manner that is culturally and contextually appropriate.
2. Be aware there may be laws in addition to standards which regulate how WSF works to them.

3. WSF will intentionally plan the data lifecycle in such a way as to not create an excessive burden on participants, carefully considering what data are needed and why; how it will be used; and how to collect only the minimum data required to accomplish programmatic aims.

C. Right to make an informed decision

Participants have the right to be fully informed in order to make a decision about their participation in any data activity.

1. WSF and its agents will gain informed and voluntary consent before obtaining any information from participants. Data will only be used for the purpose it was collected for.
2. All participants are free to choose whether or not to give their consent, without inducement or negative consequences should they choose not to participate.
3. All participants and are free to withdraw their involvement in the data activity at any stage without any negative consequences, including their participation in WSF programs.
4. If the data process involves minors, WSF will get both their and their parents' and guardians' consent, except in circumstances when it is inappropriate to do so.
5. Consent will be based on a transparent and accurate assessment about the use of data and context. If the use or the context changes, WSF will re-evaluate whether re- consent is needed.

D. Right to privacy

WSF will ensure a participant's right to privacy in the treatment of his/her data and has a responsibility to protect the identity of those providing data, unless otherwise outlined and agreed to in the informed consent.

1. WSF will ensure that, when appropriate, the process of data collection is conducted in an environment where the privacy of the participant (or group of participants in the case of focus group discussions) is upheld.
2. WSF and its agents will not discuss or share in any form, information gathered from participants with any unauthorized (by WSF) persons.
3. WSF will minimize the collection of personal data, only collecting it when absolutely essential for the data activity.
4. WSF will ensure limited access to identified data records and store them securely.
5. While WSF encourages data sharing for transparency and accountability purposes, data which are shared openly must be anonymized, unless specific consent from the participant has been obtained, and it does not place participants at risk.

E. Right to not be put at risk

WSF will not put participants in any security risk as a result its data activity. This principle is not pertinent when public officials or private sector actors who are acting in their official capacity. These individuals/ groups will be protected when acting as private citizens and not in their official capacity.

1. WSF and its agents will not collect non-essential data that could put participants at risk without justification and a clear process for managing and mitigating that risk.

2. WSF will take all reasonable measures to ensure that the process of data collection and the totality of the data lifecycle have no negative physical, psychological or political consequences for the participants. WSF will store all high-risk data securely.

3. WSF will mitigate risk to all its participants, but especially participants from vulnerable populations and groups or any participants engaged in sensitive topics/activities. Such topics must only be approached by personnel with the appropriate training and experience.

Additional Considerations

F. Gender

WSF will take particular care to use strategies that minimize or mitigate the impact of barriers to the participation of women, in order to ensure that their voices are heard and their opinions/experiences are accurately and fairly represented. Special attention must be paid to take women's particular needs into consideration during the entire data lifecycle.

G. Humanitarian Crises and Fragile States

Extra care will be taken with data collection in humanitarian conflict responses and fragile states. It is imperative that if data will compromise a person/s safety, those data should not be collected. In extreme cases where access is limited or denied, remote data collection may be considered. Measures must be taken to store data safely - see section D.

Enumerators or those conducting qualitative studies should likewise be protected. Enumerators must be trained on safety procedures and have access to support. Insurance policies should be in place to cover all eventualities. All conflict responses should be seen as high risk.

Governance & implementation of the Policy

The ultimate responsibility for this policy rests with the Board. Every 3 years, the Board shall commission a review of, and seek recommendations on potential updates to, the Responsible Program Data Policy. This effort ensures that the policy remains current and relevant, given the changing context in which WSF operates. Following any updates to the policy, the set of minimum standards will also be reviewed and updated as required.

Policy implementation is the responsibility of WSF Executive Director and his/her designates. Support for policy implementation will be provided by relevant personnel within each affiliate. Every 3 years, the Board shall commission a review of compliance with the policy, and seek recommendations on potential updates to the Responsible Program Data Policy.

Glossary of terms

Anonymous data: Any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual. **Anonymised data** would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible.

Data: The physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means. Data may be numerical, descriptive or visual.

Data collector: A person or organization collecting data on behalf of the data controller.

Data controller: A party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

Data management: The development, execution and supervision of plans, policies and practices that govern data processing.

Data processing: Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Data Risk, High: High risk data includes personal data, including any information that requires privacy and security protections, where data confidentiality is required by law, policy, or contractual obligations. It also includes data collected in programmatic, environmental, or political contexts where disclosure could cause direct harm to participants or put them at risk of adverse effects.

Data Risk, Medium: Medium risk data includes business or strategic data, or any non-confidential internal data that should not be shared publically, where unauthorized disclosure could cause material loss to the organization or brand risk. Includes aggregated data.

Data Risk, Low: Includes public data and data collected in low risk contexts, or information and programmatic, environmental, or political contexts where disclosure would not involve any risk to participants (would cause no adverse effect).

Data subject: The formal term for any individual who is the subject of personal data. See **participant** for an expanded definition.

Informed consent: A process for getting willing permission to collect data of any kind based upon a clear appreciation and understanding of the facts, implications, and consequences of any engagement from participants.

Participants: A preferred term for data subjects, expanded to include any group, cooperative, or other entity with which WSF works that provide program data.

Personal data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Program: A set of strategically aligned, mutually reinforcing interventions – by WSF and others –that contributes to sustained, positive impact on poor people's lives. For the purposes of this document, Programs are understood to be those that are defined as such in the Strategy.

Project: A group of activities or interventions with a well-defined target group and period for implementation aiming at achieving a set of outputs or outcomes that will contribute to bring about changes in people lives. They are designed and implemented by one or several partners, which might include WSF itself, and are aligned through outputs, outcomes or objectives to an overarching program.

Responsible data: The duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data while respecting the values of transparency and openness.

Transborder flows of personal data: Movements of personal data across national borders.