Responsible Data Use Principles

This document outlines the guiding principles for the responsible use of data by Search for Common Ground (Search), its employees, partners, and contractors. Its intent is to outline the values that should guide organizational decision-making, programmatic policies, and individual conduct in relation to the handling of data, especially data collected on human research subjects or program participants.

A key component of Search's Do No Harm policy is the responsible and ethical use of data. Search is committed to doing no harm through the implementation of programs, research, or evaluation. Search programs take great care to understand how activities might negatively affect intended participants or their communities. Given the complex and dynamic environments in which Search operates, laws and regulations applicable to the ethical and responsible use of data may not exist or may vary widely by context.

Search's responsible data use principles are organized into six thematic groups: Respect for Individual Autonomy, Justice & Fairness, Privacy & Fair Information Practices, Transparency & Accountability, Third Parties & Partners, and Risk Assessment, Risk Mitigation & Security Measures. These principles are informed by international data security standards, regulatory frameworks (e.g., the EU's GDPR or the Principles for Digital Development), and best practices for INGOs.

Respect for Individual Autonomy

People are People

Provide human beings respect and dignity whether they are sitting in front of you or represented as numbers on a spreadsheet.

Informed Consent

Program participants and research subjects must understand the potential risks of their participation, what data is being collected, why it is being collected, how it will be used, and how it will be protected. Consent must be affirmative and continual; the consenters must understand that their participation is completely voluntary and they may leave at any time. Informed consent means that participants/respondents understand their rights to access, delete, block, or amend their data.

Recognition of Power Differentials

Data collectors should be mindful of the power they wield due to differences in perception or culture (e.g., gender, race, origins, age, or city of origin), especially as this relates to informed consent. The location of data collection may also contribute to power imbalance or bias as participants may feel unsafe or pressured to respond. Data collectors should assess whether the use of monetary or material incentives would constitute an imbalance of power that undermines the voluntariness of the informed consent process.

Justice & Fairness

Non-discrimination

The protection and storage of data should not discriminate in any way; all respondents are due equal respect. Data collection efforts should not discriminate without a justifiable research-oriented purpose (e.g., a survey that only targets rural women because the program is designed for rural women).

Consideration of Vulnerable Populations

Data collection should always consider how the effort includes underrepresented/marginalized populations.

Privacy & Fair Information Practices

Data Minimization

Do not collect more data than necessary for the identified research/evaluation purpose. Avoid collecting personally identifiable information (PII) unless it is necessary. . For example, it may be necessary to collect the names, phone numbers, or emails of participants in a training in which follow up and communication between trainees and implementing staff are necessary, whereas collecting similar PII while conducting randomized household surveys may be entirely unnecessary.

Collection Limitation

Limit the number of respondents and questions to what is necessary for the research/evaluation purpose. Well-designed qualitative research should reach a saturation point, and quantitative instruments should sample a small, representative subset of the population.

Retention Limits & Disposal

Establish a time window within which the data will be stored and then safely discarded.

De-identification

Anonymize data in all cases unless there is a specific research/evaluation purpose for including PII.

Data Quality

Collecting and storing quality data reduces the need for additional data collection, leads to quality analysis, and respects the dignity of respondents by accurately representing their data.

Transparency & Accountability

Compliance

All programmatic and research activities will comply with relevant legal and regulatory frameworks regarding data security, personal privacy, and research ethics. Teams and individuals must ensure that applicable laws in their context are respected and upheld.

Oversight

No single data collection, management, or analysis effort should be handled entirely by one person. Teams should conduct checks for data quality, storage safety, and analysis accuracy and hold each other accountable to uphold Search's responsible data use principles.

Third Parties & Partners

All third parties, contractors, partner organizations, and sub-grantees are expected to uphold the same responsible data practices, comply with all applicable laws and regulations, and notify Search of any lapses in compliance. If lapses are identified, Search will take appropriate measures to address them.

Risk Assessment, Risk Mitigation & Security Measures

Design for Security

All activities with data components should be designed with security in mind. Projects with large data collection components should consider drafting and implementing a responsible data use protocol document.

Effective Risk Modeling

All data-related activities should be designed to incorporate risk models that comply with best practices for INGOs. The design phase should include a detailed plan that examines the project's assets, adversaries, and vulnerabilities, which are then clearly linked to mitigation strategies.

Data Storage

For all activities that include data collection, safe storage must be ensured, including preventing third-party access. All stored data must be destroyed after a maximum of 10 years. No data should report names or other information that would identify respondents.

All data collection, management, and analysis efforts should begin with an assessment of potential risks to the people represented in the data, especially if it includes PII.