Handout 6. Responsible Use of Data Collection & Management Technology

www.salanga.org

Responsible Data is a holistic concept that includes attention to data management at every step of the project cycle.

Humanitarian and development practitioners collecting and communicating project data are facing a shifting technological and political terrain. It is important to build up knowledge in responsible data practices in order to effectively identify and minimize risks to organizations and to project participants, and to develop plans for collecting, handling and communicating project-related data.

The "Do No Harm" practice in projects needs to be expanded to include the digital, physical, and psychosocial aspects related to data security.

Mass amounts of data are now easier to collect and archive. While digital data collection methods and tools are designed to increase efficiencies and data accuracy, donors are also demanding more data collection and analysis for funded projects. This has led to a situation where significant amounts of data are collected, produced, and made available by organizations. However, organizations and staff may not be fully aware of how to responsibly protect data.

Project design rarely considers what information needs to be stored, the metadata that is automatically collected, and which actors will have access to this data. Organizations need to clarify up front what data will be shared, from whom and with whom and under what circumstances and conditions, and detail out the responsible maintenance, retention or destruction of data.

Data Lifecycle

Data lifecycle describes what happens to data across a project cycle, from the collection and storage of data, through to the analysis, reporting and sharing of data. Responsible data management principles and practices should be incorporated into every stage.

Informed Consent

Standard components should include:

- easy-to-understand explanations of the purpose of the data collection
- why respondents have been invited to participate
- the voluntary nature of participation
- the time it will take to participate and the form participation will take
- benefits and risks from participation in data collection
- the types of data to be collected
- how the data will be stored and analyzed
- with whom it will be shared
- the intended uses of that data
- how confidential and anonymous respondents' data are
- the possibility of withdrawing consent at any time
- contact information of someone leading the study, should respondents have further questions or concerns.

SPUR CHANGE Capacity-Building & Knowledge Sharing for Small and Medium Organizations (SMO) | inter-council network Provincial & Regional Councils for International Cooperation | Global Affairs Canada | Affaires mondiales Canada | salanga

Confidentiality means that the project team (or designated staff members) may know the identity of the responders, however, they commit to certain principles to keep everything they learn confidential within the project team. This commitment of confidentiality may be voluntary or legally required, depending on the circumstances and context of the purpose of data collection. Confidentiality is a scale, from where all data collected is public, to where all data (and results from data) are fully confidential and cannot be shared beyond the designated individuals.

Confidentiality is a must if we want to ensure that respondents answer truthfully, especially as regards power relations.

Anonymity is the degree to which the respondents can be connected to the answers we recorded. This means that specific measures were considered to ensure that the responses (data) cannot be traced back to the respondents. Anonymity can be achieved by removing from the data collection or data set any responses or variables that could lead to the ability to trace answers or data to individual respondents. Anonymity is also a scale from where responses/data are easily traceable to individual respondents (e.g. contains names) to where responses/data are completely anonymous and cannot be matched with respondents.

Anonymity is desirable in data collection, because it can limit the damage caused by an unauthorised data leak. Note that even if names are not disclosed, attention needs to be paid to the other ways in which respondents might be identified. For example, age, gender and the name of the community might be enough to identify someone in a small community.

Data Safety refers to the physical existence of data (on which medium—hard copy and/or electronic, and where the data is stored), the ability to store it and access it over a period required for data usage, how access to the data is managed, and legal requirements to maintain certain data for a certain period. Tips:
- Plan for what will happen after the project, and when the data will be deleted permanently
- Consider backing up the data off-site.

Data Security refers to the human-caused threat to the data (e.g. unauthorized access to the data; intention to prevent you from accessing your data). Tips:
- Use technologies and apps that ensure encryption
- Use a password manager tool
- Secure the organization's and your personal computers.
- Carefully read the terms and conditions provisions of the services you use.

Responsible Use of Data Collection & Management Technology

www.salanga.org

CHECKLIST

Key Questions for Responsible Use of Data Collection and Management Technology

1 PURPOSEFUL COLLECTION

What data will you collect and how?

- ☐ We have a clear vision for why we want to undertake the research and how data will be used
- ☐ Only information that is necessary for the project scope is being collected
- ☐ Informed consent has been given by each respondent prior to data collection
- ☐ High priority is put on data anonymization
- ☐ It is culturally appropriate to use the selected technology with the respondent group

2 RESPECTFUL ENGAGEMENT

Who will you collect data from?

- ☐ Use of data collection technology will not cause any harm to vulnerable groups
- ☐ The ways in which respondents are potentially vulnerable are described

3 DATA STORAGE

Where will you store the data?

- ☐ Risks and benefits of different kinds of storage were considered (physical; offsite servers; cloud storage)
- ☐ Responsible data practices are considered along the entire data lifecycle
- ☐ Rules are established for data handling in the long term *(How long will data be kept; information is encrypted…)*

4 DATA ACCESS

Who will have access to the data?

- ☐ Roles are defined around who will have access to what kinds of data
- ☐ Terms of use are developed for data shared with third parties
- ☐ Different levels of data permissions are assigned to different categories of people
- ☐ Everybody with access to data has a good understanding of data security
- ☐ Rules are in place to ensure data will not end up in the wrong hands

This document was adapted from the Responsible Development Data – Practitioner's Guide (V1) [https://responsibledata.io/]

SPUR CHANGE Capacity-Building & Knowledge Sharing for Small and Medium Organizations (SMO) | inter-council network | Global Affairs Canada | Affaires mondiales Canada | salanga