Protection Policy

***Spatial data and mapping activities have the potential to create risk or cause harm to people and communities. HOT, as an agency both carrying out and supporting mapping activities and creating open, freely available spatial data with few constraints on its use, is responsible to understand, assess, mitigate, and protect against risk and harm arising from activities we undertake or support.***

This policy lays out the ways in which stakeholders in data collection activities, data storage, and data use can approach these responsibilities, and represents HOT’s commitment to responsible, ethical practices to protect people from harm.

Contents:

[**Application and Practical Implementation**](#_usfq7x6bmxv6) **2**

[**Definition and Scope (brief)**](#_mcnjnc24elrm) **2**

[In scope:](#_8rozshk7l988) 3

[Out of scope:](#_3e51mnpcbll8) 3

[**Required Steps Before Starting Open Mapping Projects**](#_yn30vyrqnb79) **4**

[**Dissemination, Training, and Monitoring**](#_324mdsfo1l6g) **5**

[**Annex 1: Detailed Scope**](#_j1yxdol1queb) **6**

[In scope:](#_2o7gvi6gymz2) 6

[Out of scope:](#_mpa1cp4yjmv7) 6

# 

# Application and Practical Implementation

**The** [**Data Ethics and Protection Tool**](https://docs.google.com/spreadsheets/d/1sa3umVxfSBsqWxVpP8HjYOS0rwYsuHgPDfMIhSMtlnM/edit?usp=sharing) **is the primary vehicle for the implementation of this policy**. All field mapping projects, activations, and remote mapping projects in conflict/high-risk areas must complete this tool prior to beginning activities (remote mapping projects in peaceful, stable areas do not need to complete this tool).

However, this document is not intended to create obstacles to normal work or add bureaucracy. For most HOT projects (in peaceful contexts, not dealing with sensitive data), the exercise is expected to take no more than 1 hour.

**All Senior Managers and Directors within HOT** **must be familiar with this document**, and be aware of the circumstances in which activities, projects, and data must be assessed for potential harm. Managers dealing with risky contexts such as conflict zones must also be familiar with it.

It is essential that when anyone within the organization is concerned about Protection risk, this document, and the guidance and tools that support it, must be discoverable and available to them. Furthermore, in any case where Protection risk is likely to arise (such as mapping in conflict zones), the **Director(s) responsible for the projects** (normally the Hub Directors, but in cases of projects managed by Global team members, the **Senior Manager or Director** in the hierarchical line of management) are **responsible for ensuring that this policy is consulted**.

# Definition and Scope (brief)

The word “Protection” is used here in a way similar to its [common usage in the humanitarian field](https://www.unocha.org/es/themes/protection), which encompasses two basic definitions:

1. Protect the lives, livelihoods and dignity of affected people, and
2. Ensure that our own actions do not lead to or perpetuate discrimination, abuse, neglect or violence.

In humanitarian or conflict settings, both definitions apply. However, in peaceful, stable development contexts (as opposed to humanitarian or conflict settings), the emphasis is on definition 2, which can be summarized by the common injunction, “***First, do no harm****.*[[1]](#footnote-0)”

## In scope:

* Risk of harm to *people and communities that are being mapped, or about whom data is being collected* (as opposed to staff and mappers) during data collection and mapping activities, or resulting from the use and analysis of this data. This covers HOT’s own activities, projects directly supported by HOT or using HOT’s infrastructure, and any data being made available via open data platforms such as OpenStreetMap

## Out of scope:

* Operational safety and security. This document’s focus is impact and risk on communities being mapped, not the safety and security of mappers. Safety and security are important, and overlap somewhat with protection, but are ultimately a separate concern.
* Risk of harm from use *by others* of FOSS software and open data, not supported or affiliated with HOT.
  + Note: this does not disclaim responsibility for the *creation* of open data that causes harm.Use by others of Free and Open Source Software (FOSS) created or supported by HOT (as opposed to using HOT’s own infrastructure).
* Data storage on private, closed, and/or proprietary systems.

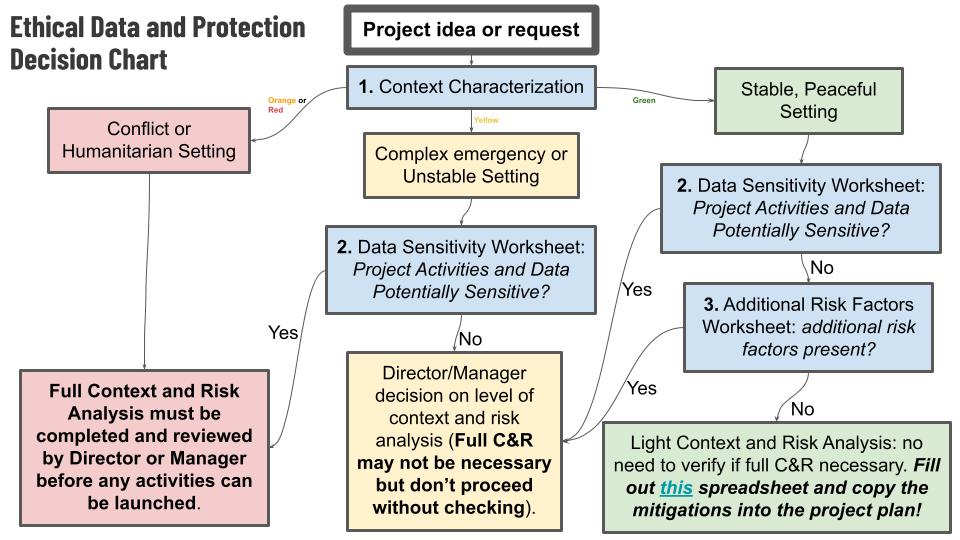
# 

# Required Steps Before Starting Open Mapping Projects

* ***All Open Mapping projects with a field component require a Protection Risk assessment.***
* ***All “Activations” require a Protection Risk Assessment as part of the size-up.***
* ***Some Tasking Manager–based remote mapping projects (primarily those in identified high-risk and/or high-sensitivity zones) require a Protection Risk Assessment.***

However, in many cases, the Protection Risk Assessment may be a very light process; this policy is not intended to impede or inconvenience “business as usual” Open Mapping.

The [**Data Ethics and Protection Tool**](https://docs.google.com/spreadsheets/d/1sa3umVxfSBsqWxVpP8HjYOS0rwYsuHgPDfMIhSMtlnM/edit?usp=sharing) contains a flowchart showing the decision tree from a project idea or request to the required level of supervision for the Protection Risk Assessment. If a project is in a Stable, Peaceful Setting, Does not involve Sensitive Data, and features no Additional Risk Factors, the risk assessment spreadsheet exercise can be conducted in one hour.



There are three categories of project, corresponding to the bottom boxes in the flowchart. In all cases, the [**Data Ethics and Protection Tool**](https://docs.google.com/spreadsheets/d/1sa3umVxfSBsqWxVpP8HjYOS0rwYsuHgPDfMIhSMtlnM/edit?usp=sharing) must be filled out. The difference between the Green, Yellow, and Red risk levels is the level of supervision required:

* **Green**: Light Context and Risk analysis required. A simple spreadsheet exercise is done by the project owner (which may be a community grantee or mentor). It is expected to take one hour.
* **Yellow**: Medium or Uncertain, Director/Manager decision on level of assessment required.
* **Red**: Equivalent to conflict zone and/or highly sensitive data collection; automatically requires Senior Manager or Director-level supervision (direct or delegated) of the Risk Assessment process prior to beginning activities.

**The mitigation measures identified in the Risk Assessment Worksheet must be incorporated into the project activity planning as Standard Operating Procedures.**

# Dissemination, Training, and Monitoring

Draft: series of workshops, seminars, external events & video

# 

# Annex 1: Detailed Scope

## In scope:

* Risk of harm to *people and communities being mapped* (as opposed to staff and mappers) from:
  + Activities undertaken directly by HOT
  + Activities undertaken by others (communities, partners etc) with *direct* support from HOT (financing, material, or in-kind support)
  + Activities undertaken using HOT’s own managed infrastructure (Tasking Manager or similar)
  + Data owned and managed by HOT
  + Data owned and managed by others that was directly derived from HOT-supported activities
  + Creation of data (Open Data or not) that a duly diligent assessment would find creates risk and/or harm to people or communities

## Out of scope:

* Operational safety and security. This document’s focus is impact and risk on communities being mapped, not the safety and security of mappers. Safety and security are important, and overlap somewhat with protection, but are ultimately a separate concern.
* Risk of harm from:
  + Use by others of [Free and Open Source Software](https://en.wikipedia.org/wiki/Free_and_open-source_software) (FOSS) created or supported by HOT (as opposed to using HOT’s own infrastructure).
    - For example, if another organization creates their own instance of the Tasking Manager, without direct support from HOT, use of HOT logos, or direct involvement from HOT, the principles of FOSS and the Tasking Manager license[[2]](#footnote-1) are clear: anyone is free to use the software, and HOT is not responsible for their conduct.
  + Use by others of [Open Data](https://en.wikipedia.org/wiki/Open_data) created or supported by HOT.
    - For example, use of OpenStreetMap data is governed by the [Open Database License](https://opendatacommons.org/licenses/odbl/), which allows any use whatsoever provided the data is attributed, shared, and kept open. HOT (or any other creator of such Open Data) is not responsible for the conduct of users.
* However, the *creation of Open Data that may cause harm* remains firmly within the scope of this policy. In a sense, once released into the world, Open Data cannot be recalled. Therefore its creation and release carries responsibilities.Information security and IT practices. While Protection implies a responsibility to properly secure sensitive data (sometimes referred to as Data Protection[[3]](#footnote-2)), this document does not prescribe how this is to be done.
  + For example, questions of how to secure passwords for Quickbooks, set permissions in Google Drive, or use 2FA on email accounts is the responsibility of the Data Security team at HOT. Questions of *what data we should even consider having, keeping on Google Drive or internal storage, or sending by email*, based on the potential of such data to cause harm, fall within the scope of this document.

1. From the Latin [*Primum non nocere*](https://en.wikipedia.org/wiki/Primum_non_nocere), a principle in both humanitarian and development work borrowed from the health field, which, as per the article in the link above, is “invoked when debating the use of an intervention that carries an obvious risk of harm but a less certain chance of benefit.” [↑](#footnote-ref-0)
2. [HOT’s Tasking Manager is licensed under a BSD 2-Clause license](https://github.com/hotosm/tasking-manager/blob/develop/LICENSE.txt), a liberal (non-copyleft) license that permits any use whatsoever of the code provided the copyright notice, conditions, disclaimer, and source code are made available with any distribution. [↑](#footnote-ref-1)
3. Though this is a narrow and incomplete definition; a more complete definition of [Data Protection is better phrased as Information Privacy](https://en.wikipedia.org/wiki/Information_privacy) and addresses questions of what data to have/create, not merely how to technically secure it. [↑](#footnote-ref-2)