Policy: Protection

Policy Type: ☒ Original ☐Addendum

Owner: Director of Data

Responsible Unit: Data

Current Effective Date: 1 November 2022

Approved by: *Currently draft - waiting for approval*

Last Updated:

Applies to:

☐ Global only ☐ All offices other than Global

☒ All offices ☐Other, please specify:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| Version | 1.0 |
| --- | --- |
| Last reviewed by: | Paul Uithol |
| Next review date: |  |

Contents:

[**Introduction**](#_6ot2mbbimyrv) **3**

[**Application and Practical Implementation**](#_rvz74xq8rt6s) **3**

[**Definition and Scope**](#_mcnjnc24elrm) **4**

[**Required Steps Before Starting Open Mapping Projects**](#_yn30vyrqnb79) **5**

[**Implementation**](#_n6nyjeiowf8p) **6**

[**Roles and responsibilities**](#_324mdsfo1l6g) **6**

[**Annex 1: Resources, training, and monitoring**](#_e3uz6fbr37ms) **8**

[**Annex 2: Detailed Scope**](#_jp7lgojs3fpa) **9**

# 

# Purpose

***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. Stakeholders include HOT staff and deployed volunteers, and can also include (OSM) communities engaging in data collection activities funded by HOT or other donors.

# 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 supported by HOT or using HOT infrastructure must complete this tool prior to beginning activities (remote mapping projects in peaceful, stable areas do not need to complete this tool).

Note 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. Project Managers dealing with risky contexts such as conflict zones must also be familiar with it.

This document, and the guidance and tools that support it, must be discoverable and available to anyone within the organization concerned about Protection risk. 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, followed, signed off, and stored along other project documentation.**

# Definition and Scope

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, “***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

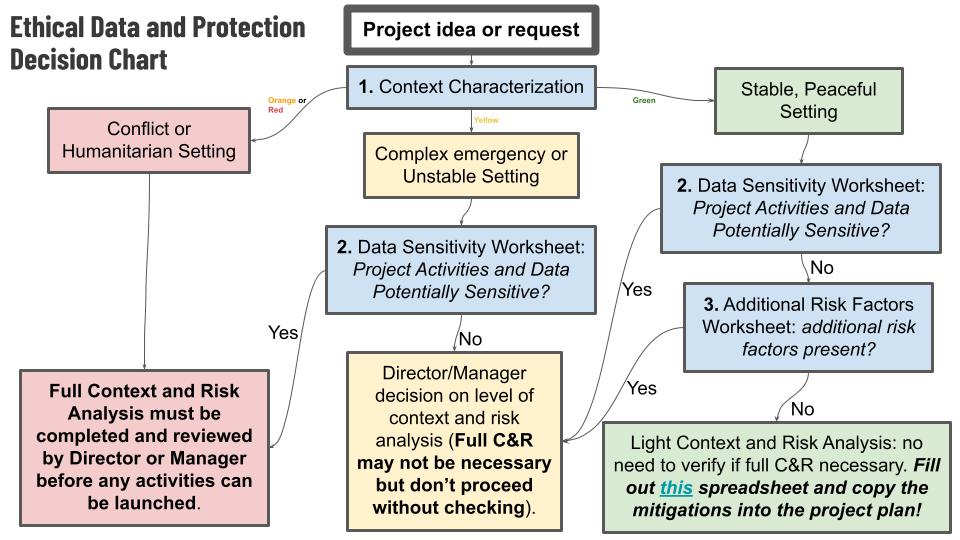
**Out of scope:**

* Operational safety and security. This document’s focus is potential impact and risk on communities being mapped as a result of creating open spatial data, not the safety and security of mappers. Safety and security are important, and overlap somewhat with protection, but are ultimately a separate concern. This is covered under the [HOT Policy: Security](https://docs.google.com/document/d/1xqQlopIQIlQG7qWIcJDWRSwuthyzT0CKeixzFwdkwwo/edit) .
* Data stored on private, closed, and/or proprietary systems operated or controlled by HOT. This will be covered under an Information Security policy.
* Non-HOT affiliated or supported open data or [Free and Open Source Software](https://en.wikipedia.org/wiki/Free_and_open-source_software) (FOSS), and risk to others resulting from its use.
  + Note: this does not disclaim responsibility for the *creation* of open data that causes harm. This pertains to use by others of Free and Open Source Software created or supported by HOT that is not running on HOT’s own infrastructure.

# Required Steps Before Starting Open Mapping Projects

* **All HOT-supported 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.

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. Rather, it can encourage a constructive dialogue about potential data use and its implications with affected communities. 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:



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. This means a project is in (a) a Stable, Peaceful Setting, (b) Does not involve Sensitive Data, and (c) features no Additional Risk Factors. 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 Director-level supervision (or Senior Manager level if delegated) of the Risk Assessment process prior to beginning activities.

Each Protection Risk Assessment consists of 5 steps, which are explained in more detail in the tool:

1. **Context Categorization:** identify the type of context. This results in a red, orange, yellow, or green context label.
2. **Data Sensitivity Assessment**: not all data has equal potential for harm, and this differs depending on contextual factors. Identify any potentially sensitive data *within the identified context.*
3. **Additional Risk Factors**: a given location may be generally peaceful and stable, but may require more than a light protection risk assessment if specific contextual factors are present, such as disease outbreaks or elections.
4. **Protection Risk Assessment**: identify specific risks by assessing vulnerability, likelihood, and impact. Create mitigations measures and project modifications based on the identified risks.
5. **Signoff and Approval**: review the filled out Data Ethics and Protection Tool. Consider if the risk level is acceptable, or if additional modifications and mitigations are required. ***If residual risk is deemed unacceptable, the ultimate consequence can be that a project should not proceed in the proposed form****.*

The completed “Data Ethics and Protection Tool” spreadsheet should be stored together with relevant project documentation in the project folder.

# Policy implementation

Organization wide:

* ~~Protection risk assessments are incorporated into an Activation’s size-up mechanism~~
* Protection risk assessments are incorporated into mapping project initiation checklists (master lists with the AMPS team and any Hub specific procedures and checklists)
* ~~SMT specific workshop~~
* Training opportunities and workshop provided to all staff

External:

* Published in curated open collaboration form (GitHub)
* Review and feedback from sector experts
* External workshops and incorporation into sector resources

Per project (see [Required Steps Before Starting Open Mapping Projects](#_yn30vyrqnb79) for which):

* Copy the template [**Data Ethics and Protection Tool**](https://docs.google.com/spreadsheets/d/1sa3umVxfSBsqWxVpP8HjYOS0rwYsuHgPDfMIhSMtlnM/edit?usp=sharing)
* Execute the steps associated with the “Data Ethics and Protection Tool”.
* Review with the relevant Senior Manager, and decide on signoff and approval.
* Incorporate the mitigation measures identified in the Data Ethics and Protection Tool on worksheet “4. Protection Risk Assessment” into the project activity planning as Standard Operating Procedures.

# Roles and responsibilities

| Project managers | Complete Data Ethics & Protection Tool under the supervision of Senior Manager or Director, and in collaboration with the project team - in consultation with (potentially) affected communities where possible. |
| --- | --- |
| Direct supervisor of project managers (often Team Leads) | Ensure Data Ethics & Protection Tool is completed adequately, and possible risks are flagged and mitigated. |
| Senior Management Team members | Provide oversight, support and ultimately accountable for responsible project implementation and execution. |
| Board | This policy is under the supervision of the Board “Risk Management” committee. |

# 

# Annex 1: Resources, training, and monitoring

* GitHub repository (public) with resources: <https://github.com/hotosm/data_protection_project/>
* [Data Ethics and Protection Tool](https://docs.google.com/spreadsheets/d/1sa3umVxfSBsqWxVpP8HjYOS0rwYsuHgPDfMIhSMtlnM/edit?usp=sharing)
* Base presentation: [Protection Framework Presentation\_base](https://docs.google.com/presentation/d/1XzexnMiMyWKldJcoZysC1AvU9YVTHGozRgbhOsfO2G8/edit)
* Presentation tailored for in person workshop: [Protection Framework Presentation\_in person](https://docs.google.com/presentation/d/1gXzlMD4l-dae8lL8N4wunMRqtaThfR2JKI4ZrTI_Fj8/edit)

Workshop materials:

* Base presentation: [Protection Framework Presentation\_base](https://docs.google.com/presentation/d/1XzexnMiMyWKldJcoZysC1AvU9YVTHGozRgbhOsfO2G8/edit)
* Presentation tailored for in person workshop:[Protection Framework Presentation\_in person](https://docs.google.com/presentation/d/1gXzlMD4l-dae8lL8N4wunMRqtaThfR2JKI4ZrTI_Fj8/edit)
  + Print handouts of the scenario slides (31-35), and the four parts of the [PLEASE\_COPY\_Data\_Ethics\_and\_Protection\_Tool](https://docs.google.com/spreadsheets/d/1sa3umVxfSBsqWxVpP8HjYOS0rwYsuHgPDfMIhSMtlnM/edit): Context Categorization, Data Sensitivity Assessment, Additional Risk Factors, Protection Risk Assessment.

Materials still to create:

* Video recording of virtual workshop

Training events:

| **When** | **Where/who** | **Facilitators** |
| --- | --- | --- |
| 14 Jul 2022 | ESA Open Mapping Grant mentors | Shamillah Nassozi & Michael Otieno |
| 22 Aug 2022 | State of the Map Florence | Shamillah Nassozi & Jessie Pechmann |
| 19 Oct 2022 | SMT | Ivan Gayton & Paul Uithol |
| 25 Oct 2022 | GeONG | Paul Uithol & Shazmen Mandjee |
|  |  |  |
|  | **Planned:** |  |
| Jan 2023 | All staff meetup - workshop | Shamillah, Paul, Shazmane, Ivan |

# Annex 2: 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)