HOT Humanitarian
OpenStreetMap
Team

1100 13th Street NW, Suite 800
Washington, DC 20005 USA
info@hotosm.org
www.hotosm.org

Policy: Protection

Policy Type:	☒ Original	☐Addendum
Owner:	Director of Data	
Responsible Unit:	Data	
Current Effective Date:	1 November 2022	
Approved by:	SMT	
Last Updated:	1 October 2023	

Applies to:

☐ Global only ☐ All offices other than Global

☒ All offices ☐Other, please specify:

Version	1.2
Last reviewed by:	Paul Uithol, Jessie Pechmann
Next review date:	June 2024

Version history:

Final draft	3 June 2022	Final draft proposed for adoption by SMT
1.0	1 November 2022	First approved version
1.1	1 June 2023	Address comments from external review
1.2	1 October 2023	Clarity of review and approval process.

Contents:

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

HOT's approach to ethical data is informed by the Data Principles[1] of "**Open and accessible**", "**Useful and usable data**", "**Inclusive and representative**", and "**Ethical data and protection**". Specifically, "**Ethical data and protection**" means that HOT aims for the most meaningful collaboration in data management and planning with the people and communities we work with, and to uphold policies and guidance to minimize risk of harm, including impact assessments and informed consent for any data collection or use. This includes the following four tenets:

1. Apply a workable process of **engagement and informed consent** across our activities, including for remote sensing and digitization (while accounting for an ever more sophisticated technological landscape).
2. Ensure **respect** for the beliefs, cultures, lifestyles, and **choices of communities in the decision making around data collection and sharing**, and in our use of collected information. Engage partners in the ethical use of information.
3. Conduct **risk and data impact assessments** to assess and minimize risk of harm for all projects together with the relevant communities. In situations where conflict is a factor, follow the "Conflict zones mapping policy".
4. Ensure **everyone at HOT is compliant with the application of data and protection principles**.

See Policy: HOT activities & mapping in conflict zones for more information for mapping in conflict zones.

[1] https://www.hotosm.org/updates/data-principles/

2. Application and Practical Implementation

The Data Ethics and Protection Tool 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 less 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.**

3. Definition and Scope

The word "Protection" is used here in a way similar to its common usage in the humanitarian field, which encompasses two basic definitions:

1. Protect the lives, livelihoods, safety, health, 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.***[2]"

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 (financing, material, or in-kind support) or using HOT's infrastructure (Tasking Manager or similar),
  - any data being made available via open data platforms such as OpenStreetMap,
  - any data HOT owns or manages (open data or not) that a duly diligent assessment would find creates risk and/or harm to people or communities,
  - and finally data owned and managed by others that was directly derived from HOT-supported activities.

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 .

[2] From the Latin *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.".

Sometimes, this maxim is expanded to "Do no *further* harm" - acknowledging that humanitarian work is more or less by definition in contexts where harm is already prevalent, and the imperative is to minimize the risk of further harm from our interventions, in balance to their benefits.

- Data stored on private, closed, and/or proprietary systems operated or controlled by HOT. While Protection implies a responsibility to carefully consider what data should be collected and stored, prescribing how to properly secure any resulting sensitive data (sometimes referred to as Data Protection[3]) will be covered under the Information Security policy.
- Use by others of Free and Open Source Software (FOSS) created or supported by HOT that is outside of HOT's control and infrastructure. Licensing on these softwares[4] are clear: anyone is free to use the software, and HOT is not responsible for their conduct.
- Use by others of Open Data that is contributed or supported by HOT. The use of OpenStreetMap data is governed by the Open Database License, 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.

Note that none of these disclaim responsibility for the *creation* of open data that may cause harm. In a sense, once released into the world, Open Data cannot be recalled. Therefore its creation and release carries responsibilities.

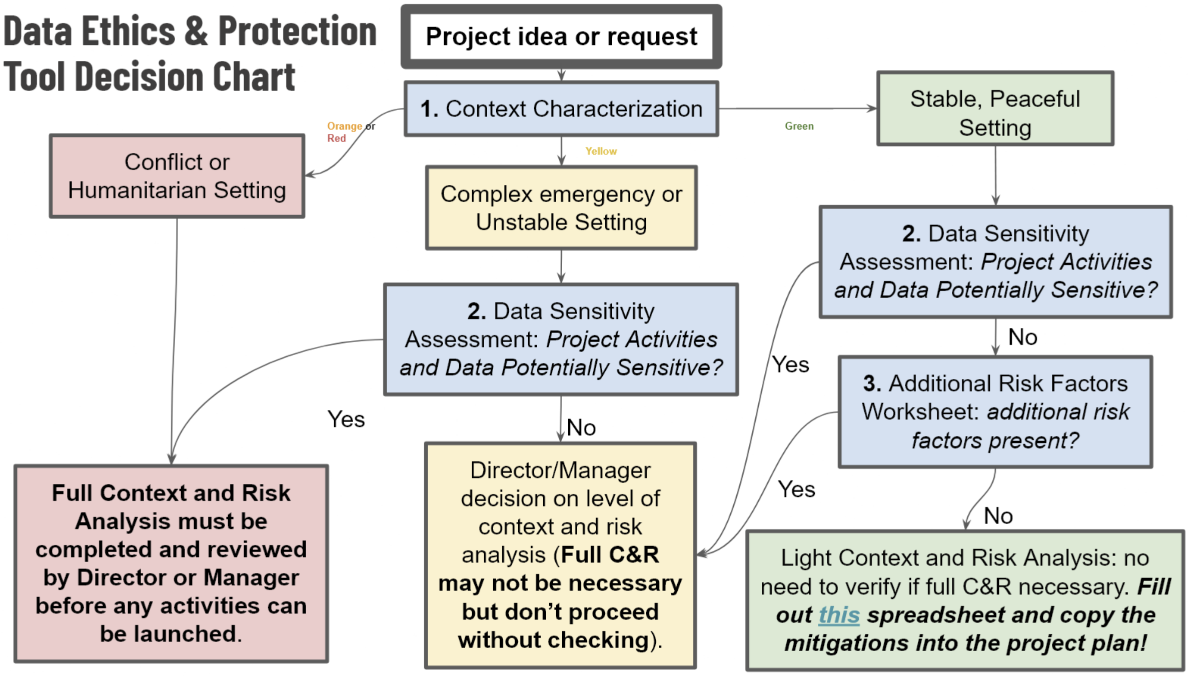
[3] Though this is a narrow and incomplete definition; a more complete definition of Data Protection is better phrased as Information Privacy and addresses questions of what data to have/create, not merely how to technically secure it.

[4] HOT's Tasking Manager is licensed under a BSD 2-Clause license, 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.

4. 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 contains a flowchart showing the decision tree from a project idea or request to the required level of supervision for the Protection Risk Assessment:


Data Ethics & Protection Tool Decision Chart
Project idea or request
1. Context Characterization
Orange or Red
Yellow
Green
Conflict or Humanitarian Setting
Complex emergency or Unstable Setting
Stable, Peaceful Setting
2. Data Sensitivity Assessment: Project Activities and Data Potentially Sensitive?
2. Data Sensitivity Assessment: Project Activities and Data Potentially Sensitive?
Yes
No
Yes
No
3. Additional Risk Factors Worksheet: additional risk factors present?
Yes
No
Full Context and Risk Analysis must be completed and reviewed by Director or Manager before any activities can be launched.
Director/Manager decision on level of context and risk analysis (Full C&R may not be necessary but don't proceed without checking).
Light Context and Risk Analysis: no need to verify if full C&R necessary. Fill out this spreadsheet and copy the mitigations into the project plan!

There are three categories of project, corresponding to the bottom boxes in the flowchart. In all cases, the Data Ethics and Protection Tool 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 or 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.

For projects in the **Yellow** or **Red** categories, the full process is to be completed and approved by the directly supervising Director. Before commencing on the actual Risk Assessment, add project relevant data for the assessment and reviews on the tab named "**0. Proposal and Scope**". Each 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. **CHECKLIST and Approvals**: 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.* There are two levels of approval:
    a. **Review**: depending on the confidence in the assessment of the staff completing the risk assessment, please request either one or two people from the protection focal points or someone familiar with the context to review the full assessment, and provide comments and suggestions. If satisfactory, reviewers should sign off.
    b. **Approval**: in principle, final approval must be provided by the Director directly supervising the staff member that is completing the Protection Risk assessment, which should be a member of the team that is to implement and execute the proposed activities. Approval of the assessment has to sit in the same hierarchy as project implementation and execution to ensure meaningful oversight of the proposed mitigation measures is possible, and require reevaluation when

necessary. In exceptional circumstances, and in close coordination, this authority may be delegated to another Director or Senior Management Team member. For final approval, please:

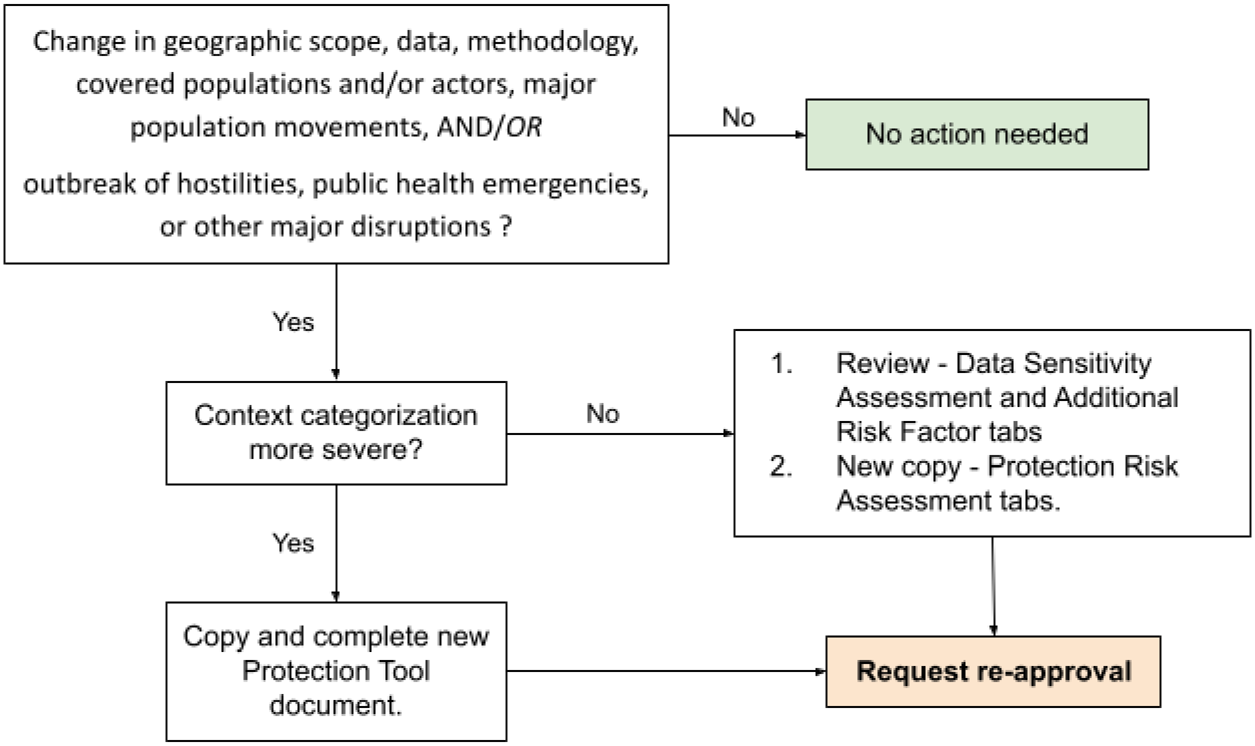
i. Review the risk assessment for any possible gaps.
ii. Review mitigations for the clarity of implementation based on feasibility, capacity, clear ownership, and effectiveness.
iii. Ensure understanding of all risks and mitigations to direct future work and answer possible questions surrounding the project.

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

5. Revisions and versioning

Over time, changes in project scope, area of operations, partner requests, or local circumstances can mean that a Data Ethics & Protection assessment becomes outdated and needs to be revised. An assessment needs to be revised in the following circumstances:

- If there are significant changes in project scope, such as the area of operations covered in data collection and mapping, the types of data collected, or the methodology.
- Additional partner requests for mapping which expand covered actors, affected populations, or data that's being requested.
- Population movements at a scale large enough to affect community dynamics and risks.
- Outbreak of hostilities, public health emergencies, or other major disruptions.


Change in geographic scope, data, methodology, covered populations and/or actors, major population movements, AND/*OR*
outbreak of hostilities, public health emergencies, or other major disruptions ?
No
No action needed
Yes
Context categorization more severe?
No
1. Review - Data Sensitivity Assessment and Additional Risk Factor tabs
2. New copy - Protection Risk Assessment tabs.
Yes
Copy and complete new Protection Tool document.
Request re-approval

If any of these occur, reassess the first step: "**1. Context Categorization**". If none of these occur, it is still recommended to periodically reassess the Context Categorization on at least a semi-annual basis. Based on the reassessment, do the following:

1. **If the Context Categorization** decision tree outcome **is unchanged** (still red/yellow/green), **or has decreased** in severity, the current assessment can be amended as follows:
   a. Review the tabs "2. Data Sensitivity Assessment" and "3. Additional Risk Factors", and update as necessary.

b. To preserve the previous risks and mitigations, rename the current version of “4. Protection Risk Assessment” to the date of its original approval - for example, “4. Protection Risk Assessment_11 March 2023”

c. Create a new copy of the tab “4. Protection Risk Assessment”in the current tool, and amend it with the date of the new assessment - for example, “4. Protection Risk Assessment_20 June 2023_latest”. Complete the new risk assessment.

d. **Request re-approval of the assessment** and note so explicitly with a new set of sign offs on the “CHECKLIST and Approvals” tab.

2. **If the Context Categorization** decision tree outcome **has increased in severity** - moved from green to yellow, or from yellow to red - a full new assessment is to be created.
   a. Date the old document - for example, “Data Ethics and Protection Tool_Somalia drought response_11-03-2023”.
   b. Create a fresh copy of the **Data Ethics and Protection Tool**, and repeat the process as laid out in 4. Required Steps Before Starting Open Mapping Projects. Date and version the new document - for example, “Data Ethics and Protection Tool_Somalia drought response_20-06-2023_latest”
   c. Request review and approval of the updated assessment.

6. Roles and responsibilities

Role	Tasks	Responsibility
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.	● Completing the tool and risk assessment ● Risk identification ● Adequate information search and consultation ● Provide an honest, fair, and accurate representation ● Request timely review and approval
Direct supervisor of project managers (often Team Leads)	Ensure Data Ethics & Protection Tool is completed adequately, and possible risks are flagged, mitigated, and incorporated into project implementation and execution.	● Supervise project planning and implementation
Reviewers	Review completed assessments based on experience and familiarity with the risk assessment process, contextual factors, and/or conflict settings. A regular pool of reviews will be selected and communicated.	● Review of completed assessments
Senior Management Team members	Provide oversight, support and ultimately accountable for responsible project implementation and execution.	● Sign off and approval of completed and reviewed assessments ● Oversight of application and implementation
Board	This policy falls under the supervision of the Board "Risk Management" committee.	● Ensure integration of prevalent risks into risk register

7. 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~~
- □ Public launch

Per project (see Required Steps Before Starting Open Mapping Projects for which):

- Copy the template **Data Ethics and Protection Tool**
- 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.

Annex 1: Resources, training, and monitoring

- GitHub repository (public) with resources: https://github.com/hotosm/data_protection_project/
- Data Ethics and Protection Tool
- Base presentation: Protection Framework Presentation_base
- Presentation tailored for in person workshop: Protection Framework Presentation_in person

Workshop materials:

- Base presentation: Protection Framework Presentation_base
- Presentation tailored for in person workshop: Protection Framework Presentation_in person
  - Print handouts of the scenario slides (31-35), and the four parts of the PLEASE_COPY Data Ethics and Protection Tool 27-04-2023_latest : 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
11 Jan 2023	All staff meetup - workshop	Paul Uithol & Ivan Gayton
1 Oct 2023	All staff training	Jessie Pechmann, Paul Uithol, Ivan Gayton and Protection Focal Points