



Using social media in CBP - Chapter 2

# Risk Assessment

# Introduction

This chapter focuses on how to get a preliminary understanding of the risks associated with using Social Media for Community-Based Protection. It covers the various steps of a CBP Social Media Risk Assessment, from understanding the risks to finding mitigation strategies.



## Resources

- [UNHCR, Policy on the Protection of Personal Data of People of Concern to UNHCR](#)
- [UNHCR, Guidance on the Protection of Personal Data of People of Concern to UNHCR](#)
- [UNHCR, Data Protection Impact Assessment Template](#)
- [ICRC, Handbook on Data Protection in Humanitarian Action, 2nd edition 2020](#)
- [ICRC & Privacy International, The Humanitarian Metadata Problem: Doing No Harm in the Digital Era, 2018](#)

While the choice of platform will depend on the preferences of the persons of concern in any given operational context, the decision should be balanced with detailed Risk Assessment.

The use of Social Media for protection brings considerable risks that must be evaluated, taking into account UNHCR's duty to protect, respect of the "Do No Harm"<sup>24</sup> principle and commitment to a rights-based approach.

Risks associated with Social Media can be grouped as follows:

1. Risk to persons of concern, including local host communities (to their safety, security and fundamental human rights, including access to asylum and freedom from refoulement, access to essential services and privacy);
2. Risk to UNHCR and partners' staff; and
3. Risk to UNHCR as an organization.

<sup>24</sup> See also [RAND Corporation, Crossing the Digital Divide Applying Technology to the Global Refugee Crisis, by Shelly Culbertson, James Dimarogonas, Katherine Costello, Serafina Lanna, 2019](#)

This chapter focuses on risks to persons of concern and host communities. UNHCR staffers are expected to know how to protect themselves and partners, and UNHCR as an organization, from risks associated with using Social Media, also covering aspects such as ICTs and information technology. The same methods you use yourself will apply when using Social Media for protection.

The risk assessment looks at the roots of these risks, as follows:

|    |                                                               |                                                                                       |
|----|---------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 01 | Risks related to POCs' personal data                          |    |
| 02 | Risks related to the platform                                 |    |
| 03 | Risks related to the regulatory environment and national laws |   |
| 04 | Risks related to the behavior of the user                     |  |
| 05 | Risks related to malicious third-party groups/individuals     |  |

Remember that UNHCR has a wealth of resources to help you navigate these issues. The table below shows some of them.



### Important

For risks associated with UNHCR staff, partners and UNHCR as organization, if the UNHCR country operation has a risk management officer or equivalent, they are good entry point, alongside the operation's Data Controller. At regional level risk staff, external relations, ICT, DIMA and innovation staff are available to guide and advise, alongside the same functions at HQ level.



## Resources:

UNHCR/HCP/2020/2 Policy on Enterprise Risk Management. The policy is to establish Enterprise Risk Management (ERM) in UNHCR, bridging various risk management policies and formal/informal practices.

UNHCR/AI/2014/22 Administrative Instruction and Procedures for Implementation of Enterprise Risk Management in UNHCR. This defines instructions and procedures for implementing ERM in UNHCR in line with the relevant policy.

## Risk to UNHCR and partners

The risks for UNHCR staff and partners relate to digital security. Physical security may be an issue, for example if someone is associated with UNHCR because of their Social Media activity and targeted as a result; or the security of the data and information handled by UNHCR and partners, such as PoCs' personal data is compromised.

UNHCR, Operational Guidance on ICT Security. This document explains UNHCR's policy for the secure management of Information and Communications Technology (ICT), including third party risks, risks related to assets and infrastructure, physical security and ICT security incidents management.

## Risk to UNHCR as organization

Most risks associated with UNHCR as an organization, aside from privacy and data security, are of a reputational nature, related to how people see or interpret what we say on Social Media. This is normally something handled by the External Relations office.

Administrative Instructions on the Use of Social Media. This defines responsibilities for the use of Social Media by UNHCR personnel and outlines principles that should inform posts to social networks. It is for all UNHCR staff (including affiliate workforce) using Social Media in a personal or professional capacity. It should inform any use of online social networks for publishing or sharing text, photos, video, audio or other digital content.

## Data protection risks for UNHCR and partners

Data protection and humanitarian action should be compatible and complement each other. Data protection principles should never be interpreted in a way that hampers essential humanitarian work but rather serves to further its objectives, namely safeguarding the life, integrity and dignity of victims of emergencies.

The ICRC, Handbook on Data Protection in Humanitarian Action, 2nd edition 2020, builds on procedures and practices that have been established in humanitarian action in the most volatile environments, for the benefit of victims of armed conflict, other violence, natural disasters, pandemics and other emergencies (together "Humanitarian Emergencies"). Some of these procedures and practices pre-date the development of data protection laws but they all are based on the principle of human dignity and the same concept of protection that underpins data protection law.

# 1. Understanding Social Media Risks for Refugees

Along with exciting opportunities to engage communities, Social Media brings with it a number of risks and protection concerns. While it is impossible to predict and deal with all of them, knowing the risks helps us choose policies, standard procedures and actions that will identify, prevent, manage and mitigate the problems, as far as possible.

Keeping abreast of the risks and weaknesses of technology<sup>25</sup> is not easy and often persons of concern use it without knowing what implications there might be for their privacy and/or digital security. Increasingly criminal groups, such as smugglers or traffickers, and/or state actors<sup>26</sup> hack or spy on conversations taking place on Social Media or mobile phones. Some are becoming very cunning at setting up online scams and traps.



## Important

When engaging communities on Social Media, do not collect personal data unless there is a good reason to do so. Purpose specification, necessity and proportionality are at the heart of data protection principles, without which one cannot be compliant.<sup>27</sup>

The technology used for the construction and maintenance of Social Media (e.g. encryption, retention period, rights for a data subject to withdraw consent etc.) affects the protection of data and privacy. A wider protection assessment needs to consider risks arising from the way Social Media platforms are used, or planned to be used, as well as the protection environment (risk of profiling of particular groups, trolling, existing legal regulatory framework and safeguards or lack thereof).

The best way to understand Social Media risks in a given context is to start with a desk review of existing studies and reports by privacy, data protection and cyber security watchdogs. Consult partners and technical experts who work on digital engagement, cyber-security and Social Media. Also hold discussions and AGD-sensitive consultations with the communities.

The second step is to work with the data controller to conduct a data mapping and a DPIA.

<sup>25</sup> Ibid.

<sup>26</sup> See [here](#) and [here](#) for more information about the use of surveillance by state actors

<sup>27</sup> See: [UNHCR, Guidance on the protection of personal data of persons of concern to UNHCR, paras. 4.1, 4.2, 2018; Art 29 Working Group opinion on purpose limitation, 2013.](#)

## I. Assessing risks related to POCs' personal data: Data Protection Impact Assessment

Often the likeliest risks for persons of concern on Social Media are associated with sharing personally identifiable information. A recent study concluded that persons of concern expressed privacy and data protection concerns when engaging digitally due to their legal status and personal background.<sup>28</sup> Ample research on privacy and data protection infringements shows that the use of Social Media entails significant data protection risks.<sup>29</sup> The dangers and malicious actors associated with social media are multiple, ranging from targeted social engineering attacks to state-backed surveillance using commercially available spyware. For example, the geo-location of vulnerable people is a worry, as is the collection of information that may allow victims of gender-based violence to be identified.<sup>30</sup>

For this reason, the risks related to data protection fall directly under the “Do No Harm” principle. The [UNHCR, Policy on the Protection of Personal Data of People of Concern to UNHCR \(DPP\)](#) lays down rules and principles relating to the processing of persons of concern's personal data<sup>31</sup> and is complemented by [Operational Guidance](#) (DPG) that further expands on its implementation, supervision and accountability. The DPP applies to all personal data of persons of concern held by UNHCR. The processing of other data, e.g. aggregated or anonymous data, does not fall within the scope of DPP but is covered among other things, by [UNHCR's Information Classification, Handling and Disclosure Policy](#)

According to UNHCR's DPP, “when elaborating new systems, projects or policies or before entering into data transfer arrangements with implementing partners or third parties, which may negatively impact on the protection of personal data of persons of concern, UNHCR needs to carry out a Data Protection Impact Assessment (DPIA).”<sup>32</sup>

A DPIA would contain a general description of the envisaged system, project, policy or data sharing arrangement involving the processing of personal data. There would also be an analysis of the risks to the rights of data subjects in view of the circumstances and nature of the personal data processed; and the safeguards, security and other measures in place or proposed to ensure compliance with this policy.<sup>33</sup>

Keep in mind that under the DPP, “new technologies or systems, tools, modules or data processing platforms which are perceived or expected to carry inherent privacy risks should, as a matter of principle, undergo a DPIA. This includes for example two-way communication using Social Media, smart phones or bulk SMS.”<sup>34</sup>

28 Incidents reported include [profiling and targeting of the Tibetan Diaspora through WhatsApp](#); spywares used against [political dissidents outside of country of origin and targeting asylum seekers](#).

29 Incidents reported include social engineering attacks such as phishing employed via messaging apps (targeting of Tibetan diaspora via Whatsapp) [profiling and targeting of the Tibetan Diaspora through WhatsApp](#); commercially available spyware used against [political dissidents outside of country of origin](#) and for [targeting asylum seekers](#); as well as new vulnerabilities that are being regularly discovered and patched in major messaging services (eg. Whatsapp)

30 See more on the [ICRC Handbook on Data Protection in Humanitarian Action, 2020](#)

31 It is consistent with [2018 UN High Level Committee on Management Personal Data Protection and Privacy Principles](#), and other international instruments concerning the protection of personal data and individuals' privacy.

32 [UNHCR, Policy on the Protection of Personal Data of People of Concern to UNHCR, 2015](#)

33 [UNHCR, Policy on the Protection of Personal Data of People of Concern to UNHCR, 2015](#)

34 [UNHCR, Guidance on the protection of personal data of persons of concern, 2018](#) (para. 8.2.3)

UNHCR firmly recommends that personal data is never collected on Social Media unless strictly necessary. Both user-based and platform-based risks associated with social media data collection should always be assessed, for example how the data disclosed by refugees on UNHCR's Social Media pages may be used by malicious actors.

UNHCR may often not be in a position to mitigate all risks associated with the use of Social Media platforms. Engaging PoCs through Social Media entails the use of platforms and services provided by a third party with whom UNHCR may often not have a contractual relationship nor oversight, particularly regarding their processing and sharing of users' personal data with other actors. Many of these platforms are not open source, as a result of which there is limited transparency and public oversight on the data collection and sharing by the platform service providers.

In most cases where personal data of PoCs on a Social Media platform is processed by UNHCR, the technological aspect of it is under limited control of UNHCR due to absence of formalized data sharing arrangement with the platform provider (e.g. Facebook). Nevertheless, the DPIA should include an overview of all technical and procedural risks associated with the platform, and the technical and procedural mitigating measures available to UNHCR. The implications of data processing by UNHCR should always be considered carefully when determining what sort of intervention is most appropriate for engaging with communities through Social Media.



## Resource

ICRC, [Handbook on Data Protection in Humanitarian Action, 2nd edition 2020](#) (Chapter 5 on Data Protection Impact Assessments - DPIA)

## II. Assessing risks related to Social Media platforms

Every type of Social Media platform has its own architecture, bias, weaknesses and data protection rules and regulations. To assess and understand these risks, you have to look at the specifics of the platforms you are considering.

Risks that are platform-related normally have to do with the software infrastructure, functionality and features of the platform itself. These risks can be related to the data privacy<sup>35</sup> and terms of use of each platform, the possibility of creating open and/or closed channels,<sup>36</sup> the possibility of encrypting content and/or the metadata generated and shared with third parties (including law enforcement and government authorities).

No platform will guarantee you can protect people from all risks but knowing the dangers will allow you to develop your Risk Assessment and work on mitigation measures to support partners and refugees in the safe use of Social Media.

<sup>35</sup> See more [here](#).

<sup>36</sup> See [Chapter 3 Section 1](#) for more information about closed and open channels.



## Resources

To explore some of the features and risks associated with different Social Media platforms, see the resources below:

- [UNHCR, Policy on the Protection of Personal Data of People of Concern to UNHCR, 2015](#)
- [UNHCR, Guidance on the Protection of Personal Data of Persons of Concern to UNHCR, 2015.](#)
- Chapter 3 of the [ICRC Handbook on Data Protection in Humanitarian Action](#) focuses on the use of Social Media by humanitarian organizations to communicate and engage with beneficiaries. The Handbook covers the use of Social Media to identify crises and improve the humanitarian response (Chapter 6: Data Analytics and Big Data.) For Messaging Apps, you can refer to Chapter 11: Mobile Messaging Apps.
- Chapter 4 of the [ICRC, The Engine Room and Block Party, Humanitarian Futures for Messaging Apps, January 2017](#) addresses the issues humanitarian organizations face when communicating or exchanging information with local communities, and their responsibility to ensure no harm comes to PoCs. This section raises issues for consideration when organizations are assessing whether Messaging Apps can be used responsibly and effectively in a given situation.

## III. Assessing Risks related to Physical Infrastructure and National Regulatory Frameworks

Every country has its own laws and regulatory systems that govern the use of ICT. This includes the ownership of the ICT infrastructure, the laws that regulate content and user rights on Social Media and the legal safeguards and recourse available.

In general, you will have to assess three categories of obstacles in any given country:<sup>37</sup>

- **Obstacles to Access** - Infrastructure and economic barriers to access; regulation of access; legal and ownership control over internet service providers and independence of regulatory bodies;
- **Limits on Content** - Legal regulations on content; technical filtering and blocking of websites; self-censorship; the vibrancy/diversity of online news media and the use of digital tools for civic mobilization;
- **Violations of User Rights**<sup>38</sup> - Surveillance and privacy; repercussions for online speech and activities, such as imprisonment, harassment or cyber-attacks.<sup>39</sup>

37 See details about how these three elements are assessed and what they include on [Freedom on the Net](#), Freedom House's annual survey and analysis of internet and digital media freedom around the world. This project consists of research analysis, fact-based advocacy and on-the-ground capacity building.

38 For the purpose of this section of the chapter, "Users Rights" are defined as a subset of the so-called [Human Rights on the Internet](#). This refers to ways governments and non-state actors around the world restrict the rights of users online by means of surveillance, attacks to privacy and legal and non-legal repercussions for online speech and activities, such as imprisonment, harassment or cyber-attacks.

39 This also includes lack of legal safeguards and recourse - e.g. is there any legal safeguard in case of misuse of personal data by the service providers?



## Resources

[Council of Europe, Guide to Human Rights for Internet Users, Recommendation CM/Rec\(2014\)6 and Explanatory Memorandum, 2014](#)

The Council of Europe recognizes that human rights apply equally on and offline. The guide to human rights for internet users explains in user-friendly terms the rights and freedoms guaranteed to internet users by the European Convention on Human Rights. The guide was designed to educate individual internet users on their online rights, as well as to encourage governments, public institutions and corporations to assume responsibility to protect human rights online. Read also the [Recommendation of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users](#), the [Explanatory Memorandum](#) and [Safeguarding Human Rights in the Net, Thematic Leaflet](#).

UNHCR must know about these risks, especially as they apply to the particular communities it works with, and weigh them against the protection outcomes expected from engaging with persons of concern on Social Media. Protecting them from possible violation of their rights is UNHCR's job.



## Factsheet

See [Factsheet 2](#) for questions that can be asked to evaluate risks associated with physical infrastructure and national regulatory frameworks.



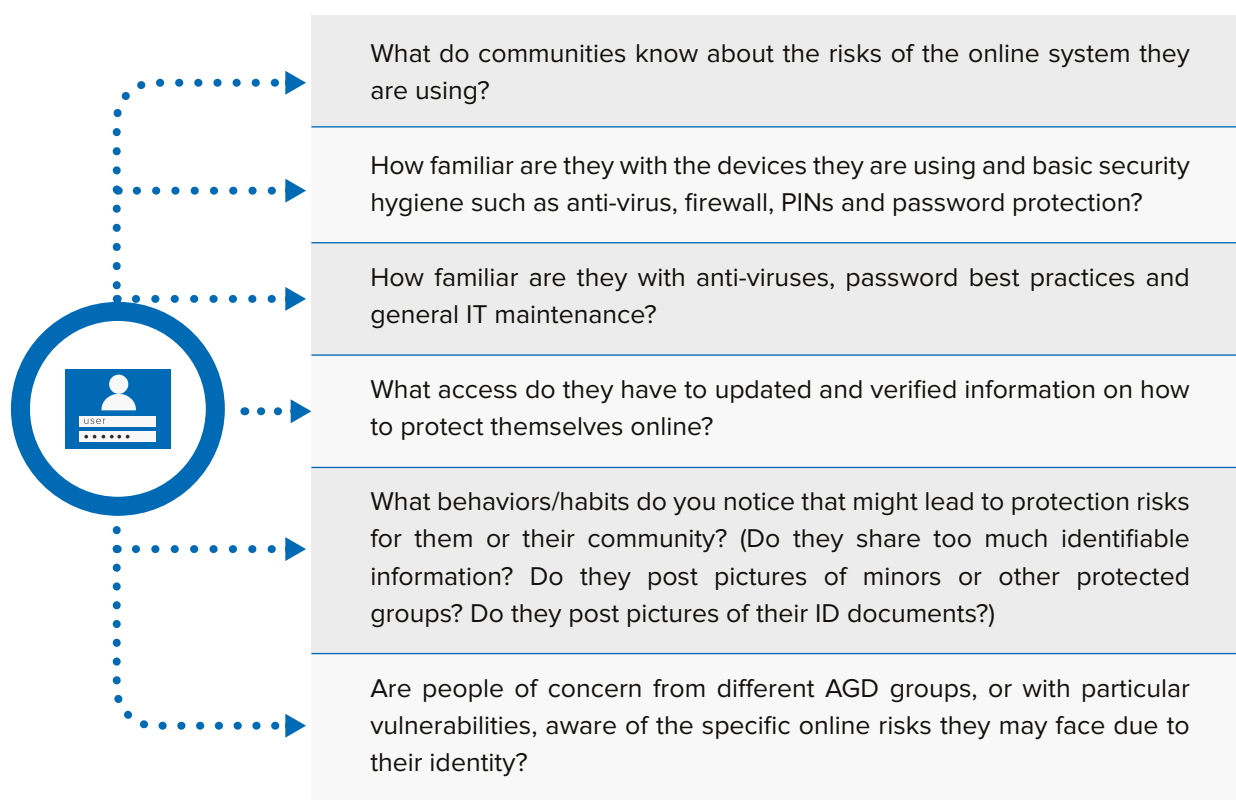
© UNHCR/Mohammad Hawari

## IV. Assessing Risks related to Users' Behavior

Our responsibility to protect persons of concern extends to actions online, and they too must understand the risks and protect themselves. Often, privacy issues and terms of use and data handling are not clearly understood by Social Media users. Refugees, IDPs, returnees and stateless people may not have much control over IT security and handling ICT equipment, including computers and mobile phones, as they may share devices or use internet cafes. And in some cases, digital literacy can be low (as a whole or for certain AGD profiles within the group).

While UNHCR staff are trained to handle and protect themselves online, persons of concern may use these technologies differently, without enough awareness of the risks involved. The questions below can guide your community discussions to see what risks they perceive online, how they protect themselves and what gaps there might be.

### Questions to understand risks associated with the behavior of users online



## V. Assessing Risks related to Third-party Malicious Actors

The risks associated with third-party malicious actors<sup>40</sup> come in two categories:



Malicious actors using Social Media in a legal way to violate PoCs' rights, for example with scams or manipulation to get them to disclose their personal information; political propaganda used to fuel conflict;



Malicious actors using illegal means such as malware infection, system compromise and social engineering attacks to harm persons of concern.

Recognizing these actors and their methods, and helping persons of concern to understand the risks, takes you a good way towards implementing effective mitigation. Exposure to harmful content, criminal networks or activities, abuse and safeguards are all covered later in this chapter.

Your assessment must investigate what types of malicious users are present on Social Media and online generally. What are the online scams? What online tools are criminals using to identify minors or other groups in order to take advantage of them? You may also want to look at groups that target specific persons of concern and find out if any groups or individuals use Social Media to spread hate, disinformation or violence.



### Important

When looking at political propaganda or incitement to violence on Social Media, bear in mind that boundaries do not really exist on the internet. In the case of refugee situations, this means that information between PoCs in the country of arrival and malicious state or non-state actors in the country of origin travels instantaneously. Online recruitment, propaganda, disinformation and hate speech are just some of the risks PoCs may encounter online. During the Risk Assessment and on an ongoing basis, make sure to monitor and assess any discrimination or hate-fueled campaigns against PoCs on Social Media, or the presence of online 'insurgency' from the country of origin. Community members affiliated with political groups in the country of origin can fuel tension and conflict with their posts.

<sup>40</sup> Malicious actors include groups and individuals operating from the country of origin (COO) and country of arrival (COA).

## 2. Analyzing Risks

Once you have identified the Social Media risks, then analyzing these risks will help you understand their likelihood and the possible consequences for Persons of Concern, UNHCR and partners.

The starting point of your risk analysis is the balance between benefit and risk . This gives clarity of purpose (what is the value of using Social Media for protection?), before diving into the risks. Now you must look for ways to maximize the benefits and minimize the risks.



### Resource

[PIM, Framework for Data Sharing in Practice , 2019](#)

This Framework identifies the various components that are necessary to support the safe, purposeful and responsible sharing of information between actors involved in a protection response. One component is the Benefit and Risk Assessment, which aims to ensure that the benefits and risks of data sharing have been systematically and collaboratively assessed, and that actions have been identified to maximize benefits and minimize risk. Although this Framework is specific to data sharing, it can help you think about data-related risks more generally.

Social media risk analysis is a process that helps determine whether advanced prevention activities are required. It enables you to set up mitigation measures and define your contingency plans. It uses scenarios to measure the likelihood of specific events/behaviors and the impact they would have on people of concern. It must always be done with a Community-Based Approach to make sure all stakeholders, offline and online, are involved.<sup>41</sup>

The [UNHCR Preparedness Package for Refugee Emergencies](#) (PPRE) promotes a standard three-step method for risk analysis, which can readily be applied to other situations and population groups:

**Step One - Scenario(s) Identification:** This process is led by community consultations, where UNHCR and/or partners discuss the risks identified in the first part of this chapter. Local partners and specialized partners who work on online rights, privacy and internet freedom will be particularly helpful when it comes to understanding the likelihood of certain risks materializing. Historical data on previous cyber-attacks or known cases of scams targeting Persons of Concern will also emerge.

<sup>41</sup> [UNHCR, Emergency Handbook, Risk analysis and monitoring - refugee emergencies, accessed June 2020](#)

**Step Two - Risk Ranking:** This process is more effective the more local partners and persons of concern are involved. Risk ranking depends on the local context and may vary over time according to a person's profile, or from location to location or topic to topic. The chances of being scammed online if you are a host community member may be low compared with those of an asylum seeker, for example. At this stage it will be important to use an AGD lens and make sure every group of the whole population you are planning to engage is involved in the ranking of risks associated with Social Media.

**Step Three - Risk Monitoring and Early Warning:** While neither UNHCR nor its partners can control how people use Social Media, we have the mandate and power to inform refugees of the risks and support them in protecting themselves. This means all protection personnel should keep up to date on how persons of concern use Social Media. How aware are they of the risks and what mitigation measures do they take?



## Resources

[UNHCR, The Preparedness Package for Refugee Emergencies \(PPRE\), A REFERENCE GUIDE FOR PREPAREDNESS, Version 3, 2020](#)

The Preparedness Package for Refugee Emergencies (PPRE) sets standards for preparing for refugee emergencies. It helps users to implement risk analysis, take minimum and advanced preparedness actions and conduct scenario-based contingency planning.

Find more information and links on how to conduct Risk Analysis and Monitoring in the [UNHCR Emergency Handbook, Risk Analysis and Monitoring - Refugee Emergencies](#)



© UNHCR/Santiago Escobar-Jaramillo

## 3 Prevention and Mitigation Strategies



### Important

Remember that the risks of engaging with PoCs on Social Media always need to be weighed against the benefits and gains, but also against the risks of not engaging at all. Protection always comes first. Serious data protection and privacy risks could be a valid reason for seeking alternative means of engagement, when the risk posed by social media use cannot be sufficiently prevented or mitigated. However, might 'not engaging' also have negative repercussions? What is in the best interests of the person of concern?

The risk assessment should be as community-based as possible, bearing in mind that UNHCR has the resources to conduct research and assess risks that are otherwise not visible to PoCs. If UNHCR decides to engage PoCs through a particular means, UNHCR owes them a duty of care to ensure the means selected are appropriate and accessible, as per the AGD Policy.

Systematic analysis of Social Media's risks helps operations decide what preventative and mitigation actions are required in each situation. Risks related to the use of Social Media need to be analyzed regularly (at least once a year) through consultation with stakeholders and the communities themselves, or whenever a change in the operational context warrants a review.

Knowing some of the factors above can help you understand how to address these risks. What education, outreach or advocacy campaign might you need to implement to support your work? A Community-Based Approach will ensure that all the actors who can influence and support the protection of refugees online are involved in the process.

Understanding how people use Social Media, and who and where malicious actors are, will help UNHCR and its partners to develop response strategies. These could include digital literacy, digital security training and digital privacy and security-awareness building. Persons of concern and local partners should be able to connect with relevant institutions to counteract criminal acts online.

Your mitigation strategy, designed with partners and PoCs, will be different in every context. Below are some activities that will help you prevent and mitigate risks:

**1. Identify, collaborate and partner with existing local networks, systems and organizations.**

These people usually know the situation well and can support UNHCR and partners in understanding the overall environment. Often, campaigns and activities are already being organized to protect user rights online, and these can be supported by UNHCR specifically for refugees, the displaced and stateless.

**2. Work with PoCs to prevent unnecessary sharing of personal information.** Always make sure you have an accessible and inclusive post pinned to the top of your Social Media account, or a banner, as the first thing visible when people open your page/account. This should

- a) alert people not to post their personal data or that of others on the platform;
- b) provide information on tools/channels that can be used for handling personal issues;
- c) explain the risks associated with using Social Media to share personal information. When people do share personal information on Social Media, always speak with them privately about why they shouldn't do it and offer alternative avenues for them to discuss personal matters;
- d) for people who share devices or access their accounts through public or borrowed devices, explain the need of signing out from accounts when they have finished. Point out the risks of sharing passwords, other log in details or personal information, or enabling others to access their accounts.

**3. Know your platforms.** UNHCR is not advised to collect and share the personal data of PoCs on Social Media. If their personal data is processed by UNHCR on Social Media, the operation's data controller is required to demonstrate full compliance with the data protection policy, including specifying the purpose for the data processing and ensuring there are legitimate grounds for it. Processing personal data should be minimized, based on the purpose and the risk. Adequate security measures should be in place, confidentiality should be respected and there should be measures to protect the data subject's rights. With regard to data privacy, each digital platform has its strengths and weaknesses. When using a specific type of Social Media platform, you need to know the possible risks connected to it.

**4. Realize the threats that will always exist.** Some people want—and will do just about anything—to get others' private information. You have to realize that you can't keep everyone's privacy secure all the time. So you must weigh the expected benefits of engagement on Social Media against the identified risks. Design appropriate and feasible prevention and mitigation strategies and be ready to change course if the risks start to outweigh the benefits or the prevention measures are no longer effective or adequate. A 'best interest' approach should be taken when considering the advantages of using Social Media in certain emergencies i.e. to ensure the immediate safety and protection of individuals.

5. **Make sure all stakeholders understand the privacy settings and terms of reference of the platforms they use.** Many Social Media sites demand users agree to their terms of use when they open a new account. These agreements are often written in impenetrable legal jargon and not available in diverse languages. Often people do not know exactly what they are signing up for. Over time, these agreements often change or are updated. Make sure you know your Social Media platforms' terms of use, including data handling, sharing and disposal, and work with partners and Persons of Concern to identify and discuss possible risks.
6. **Invest in Digital and Data Literacy.** If Social Media plays a considerable part in your interactions with Persons of Concern and if they use Social Media consistently, you may want to invest in designing and implementing - or support partners and other stakeholders in implementing - digital and data literacy training and mentoring programs. You should also be working with early adopters in communities, who play important roles in building the digital literacy of their peers and - often - older people. These activities can also promote the inclusion of more groups in online conversations, groups that can be identified via UNHCR AGD analysis.
7. **Strengthen the ability of PoCs to access Social Media platforms safely.** UNHCR believes that PoCs and communities that host them have the right, and the choice, to be part of a connected society and to have independent access to technology that enables them to build better futures for themselves, their families and the world. While the realities of providing connectivity in displacement are diverse and contextual, if you are interested in working on connectivity, make sure you connect with the UNHCR [Connectivity for Refugees](#) team.



## Resources

[UNHCR's Connectivity for Refugees initiative](#) creates safe spaces to experiment with connectivity solutions in the field. It works with UNHCR operations to develop local and context-specific, community-driven approaches to digital challenges. The UNHCR Innovation Service supports connectivity for refugees through a three-pillar approach that focuses on catalyzing connectivity innovations and solutions from the field; using research to have an all-round understanding of the intersections of connectivity and displacement; and capturing bright spots through storytelling and strategic communications.

8. **Monitor and detect emerging risks.** Monitor the risks of UNHCR engagement with PoCs via Social Media as one modality of the CBP program, looking at protection risks or violations of human rights like trafficking, surveillance, GBV, bullying and hate speech. Regularly monitoring Social Media behavior reveals links to the situation on the ground and can be used as an early warning system. The more UNHCR is able to involve PoCs themselves and partners in this activity, the better. Then monitoring is embedded in day-to-day Social Media interactions and becomes an ongoing collective effort.

## 4. Safeguarding

The use of Social Media for Protection by UNHCR staff presents a series of risks in itself, compounded by the fact that not all users have the same level of awareness of what behaviors are acceptable online.

### Protection from Sexual Exploitation and Abuse (PSEA) on Social Media

PSEA policies and practices<sup>42</sup> aim to end sexual exploitation and abuse by humanitarian workers, including UNHCR personnel, and ensure that allegations get a swift and appropriate response.

Four pillars of PSEA are stipulated in the [IASC Principals' Statement on the Prevention of Sexual Exploitation and Abuse](#), which agencies are expected to implement:

- **Manage and Coordinate:** Coordinate SEA prevention with partners and other actors, including governments, UN agencies and the private sector. Secure the commitment of senior managers to PSEA;
- **Engage with Communities and Secure their Support:** Raise PoC awareness of SEA and establish safe, confidential and culturally appropriate complaint mechanisms, designed in collaboration with them and representing different AGD groups;
- **Prevent:** Develop effective prevention mechanisms. Effective recruitment and performance management procedures are required, where the roles, responsibilities and expectations of all staff members are clearly explained. Reporting procedures for any SEA concerns should be easily accessible and staff should receive refresher orientation on them;
- **Respond:** Promote timely internal complaint and investigation procedures, led by the country's safeguarding focal point.



#### Resources

The UN Secretary-General's Bulletin on Special Measures for Protection from Sexual Exploitation and Abuse (ST/SGB/2003/13) (ST/SGB/2003/13) entered into force in the UN in 2003 and was formally adopted by UNHCR in a 2004 memorandum. On 10 May 2018, UNHCR released its [Strategy and Action Plan on Addressing Sexual Exploitation and Abuse and Sexual Harassment](#).

<sup>42</sup> See more on PSEA in [UNHCR Emergency Handbook, Protection from Sexual Exploitation and Abuse \(PSEA\)](#), accessed May 2020

When it comes to PSEA, the risks associated with using Social Media are heightened by the fact that UNHCR staff and partners have their own personal accounts, which give them access to information about People of Concern (as much as they put online). In addition, there is the option to contact and connect with them privately.

Take these steps to address possible PSEA risks online:

## Engage:

1. Raise PoCs' awareness of SEA by creating clear, multi-format content (in the right languages) that they can access online. They need to know that SEA can be as much of a problem online as offline;
2. Establish clear and confidential complaint and response mechanisms through preferred channels (or ensure a link to existing complaints mechanisms, such as call centers);
3. Tell community members how UNHCR will use Social Media to communicate with them and what they can expect in terms of response. For example, we may only discuss a certain service or we may only respond to comments during work hours). These 'rules of engagement' should be clearly visible on the platform.

## Prevent:

1. Make sure you have a monitoring system for the private and group conversations carried out via UNHCR's Social Media account;<sup>43</sup>
2. Train staff on the appropriate behavior for Social Media, both in their professional and private lives, and develop relevant SOPs;
3. Train staff on the internal pathways for reporting any concerns or suspected cases of SEA to the appropriate focal point;
4. If you use bots or automated responses or IVRs, make sure the intro message contains information on PSEA risks and how to report;
5. Always have PSEA as part of your FAQ document, if you have one.

While UNHCR will always refrain from using Social Media to collect personal data and address sensitive protection issues, persons of concern often do share their personal information online, sometimes even showing pictures of themselves or their families. For this reason, make sure your staff and partners are trained on the [Policy on the Protection of Personal Data of People of Concern to UNHCR](#).

Refer to [Chapter 4](#) and [Chapter 5](#) of this Guide to learn more about how to engage with PoCs online and how to deal with personal sharing of information.

---

<sup>43</sup> One option may be to have at least one additional user with oversight on private conversations and within closed groups. This can also reassure community members and help protect staff from potential misunderstandings or being accused of inappropriate behavior.

## Online Grooming

Online grooming is when someone uses the internet to trick, force or pressure a young person into doing something sexual - like sending a naked picture or video of themselves. Often, the groomer will build their trust before talking about doing anything sexual. Given the high visibility of UNHCR worldwide, and the widespread use of Social Media by children and teenagers,<sup>44</sup> all UNHCR staff managing and accessing Social Media must be informed about this practice and its relationship to SEA.

Regarding UNHCR, there are a number of Social Media grooming risks, from staff misrepresenting themselves to people acting under the guise of UNHCR. This is why it is essential that PoCs have access to clear and easily understandable information on the Code of Conduct for UNHCR staff.

Often working with local media helps spread information about what to expect from protection actors, both online and offline, and how to report inappropriate behavior.



### Important

The grooming of children for sexual purposes through Social Media is a growing problem. UNHCR staff accessing sensitive interfaces should be carefully vetted and clear safeguards should be established. Child safeguarding procedures for the offline world may need to be adapted online. Unfortunately online grooming often progresses rapidly, with offenders hiding behind the anonymity of the internet. The power dynamics of an offender using the 'legitimacy' of an UN-branded account should not be underestimated.



© UNHCR/Mark Henley

<sup>44</sup> Country operations should have a separate DPIA on engaging children through Social Media, also involving the Child Protection Unit. Specific SOPs should be developed.



## Resources

[UNICEF, What Works to Prevent Online and Offline Child Sexual Exploitation and Abuse?, Review of national education strategies in East Asia and the Pacific, 2020](#)

[UNICEF, Guidance for Online Child Safeguarding for Service Providers, 2020](#)

[Plan International, Working Together with Children and Young People for Safety in the Cyber-World, 2014, Guide for Plan International program practitioners who work with children and young people in programs that access and utilize ICTs.](#)



## Messaging Apps

The ICRC, together with The Engine Room and Block Party, has produced [a report](#) on the uses of Messaging Apps, such as Facebook Messenger, WhatsApp and Snapchat in humanitarian situations. The report looks at the potential of Messaging Apps to have a positive impact in crisis situations and discusses risks relating to security, data protection and privacy.

While the process of conducting a Risk Assessment for Messaging Apps is the same as explained above, several factors must be kept in mind when looking at the risks and challenges of using them for Protection. These are highlighted in the ICRC report, Chapter 4:

- Given the complexity of the systems of Messaging Apps, both new and largely untested, protection personnel should agree on codes of conduct, standards and/or ethical frameworks for their use;
- Most major Messaging App companies process and store data using proprietary systems that external organizations cannot scrutinize. If you need to address this issue, seek guidance from your regional bureau and HQ;
- Protection staff should do their best to ensure users of a UNHCR service delivered through a Messaging App are aware of and understand the App's terms of service;
- Verifying content is already an issue on Social Media. Using information from Messaging Apps can be even more challenging due to the speed at which information is sent, the volume of messages and the range of data. A Community-Based Approach to verification and content management helps mitigate this risk.

# Resourcing

Understanding all the risks and vulnerabilities associated with using Social Media for CBP in a given country is a huge task and not necessarily one that UNHCR offices can investigate alone. Luckily, support is available from the regional bureaux and HQ divisions/services, and there are a number of organizations, in each country and worldwide, that work on issues from internet privacy and freedom to the protection of children on Social Media.

Of course, it is mandatory to comply with UNHCR policies, standards and guidance, such as the Policy on the Protection of Personal Data of Persons of Concern to UNHCR. At a minimum, the risk analysis should take these into consideration.

These steps can help you maximize your resources to conduct a risk analysis of your Social Media activities:

- Try to include Social Media in your annual risk analysis, if one is done, so as to harness existing internal expertise and resources;
- Use the findings of your situation analysis to better understand the risks associated with Social Media use in the country;
- In places of high risk, consider connecting your Social Media strategy with a broader advocacy strategy, working with the government (as appropriate) and stakeholders to uphold human rights and protect PoCs online;
- Think about establishing partnerships and collaboration with local advocacy organizations already working on human rights violations online, or on the national regulatory framework for online rights violations;
- Look at existing UNHCR partners who may have the expertise or skills to address more nuanced risks, and work with them to address complex issues.



## Resource

Chapter 3 of the [ICRC Handbook on Data Protection in Humanitarian Action](#) focuses on the use of Social Media by humanitarian organizations to communicate and engage with communities. The Handbook also covers the use of Social Media to identify crises and improve the humanitarian response – see Chapter 6: Data Analytics and Big Data. For Messaging Apps, refer to Chapter 11: Mobile Messaging Apps.



## Do's

**DO** ensure fair access to information about how to use Social Media safely and securely.

**DO** engage community members to develop a better understanding of real and perceived risks on Social Media that can manifest online or offline.

**DO** seek support from UNHCR teams in understanding risk, whether related to digital access, digital engagement, data security and/or data protection.

**DO** design interventions to prevent, manage, minimize or mitigate risks presented by engaging with communities through Social Media platforms.

**DO** work with partners, including local authorities, ICT security services and Social Media companies, to highlight risks that need to be addressed.



## Don'ts

**DO NOT** overload PoCs with legal jargon. Rather, discuss with them clearly and simply the issues about their Social Media activities that may concern them directly.

**DO NOT** make perfect the enemy of the good. It is impossible to eliminate all risks but possible to manage risks sensibly, as far as resources allow. Make sure prevention and mitigation measures are in place and risk management is intelligently balanced in relation to the expected gains/benefits of using Social Media for Community-Based Protection.

**DO NOT** make assumptions about the risks communities face. Engage with them directly - especially the active Social Media users - to understand what risks are present and how they are managed (or not).

**DO NOT** act recklessly with the data of persons of concern. UNHCR has strong policies to protect their data. Complying with the policy and following associated guidance can prevent misuse and abuse.

**DO NOT** make a final decision about using Social Media without considering the potential benefits and risks of both engaging and not engaging.



## Check List

- Have you contacted the country operation's data controller to conduct a DPIA if required? ☐
- Have you shared the DPIA reports with regional and HQ DPO? ☐
- Have you contacted the regional bureau and HQ to help you conduct the risk assessment? ☐
- Have you identified and connected with in-country local actors working on online rights and SM security? ☐
- Have you conducted AGD-sensitive community consultations in readiness to discuss online risks and possible scenarios with key stakeholders? ☐
- Have you developed with all stakeholders a realistic and appropriate prevention and mitigation strategy? Have you identified ways to revise and update the strategy, and resource it? ☐
- Have you identified a process for gathering the needed consent for the use of Social Media data? ☐
- Have SOPs been developed for engaging with PoCs online, including monitoring and oversight? ☐
- Have staff and partners involved in the use of SM received basic orientation on data protection, PSEA, relevant standards and safeguarding? ☐
- Is there a system for monitoring and managing access to the data gathered and created through the SM platform? ☐
- Are SOPs in place for detecting, reporting and managing any personal data breach that would put PoCs at risk [DPP Section 4.4 and DPG Chapter 7 on Data Protection Breaches and relevant reporting procedures]? ☐
- Have you involved your data protection focal points to comply with the data protection policy, and the data controller for approval of using Social Media for specific purposes in the country operation? ☐



© UNHCR/Mohammad Hawari



## Case Studies

[Timo Luege, How Social Media is Changing Communication in Emergencies, November 2014](#)

[Anahi Ayala Iacucci, Crisis Mapping and Cybersecurity – Part II: Risk Assessment, 2011](#)

[OHCHR, The Right to Privacy in the Digital Age 2014](#)

[UN Chronicle, Government Policy for the Internet Must Be Rights-Based and User-Centred, by Wafa Ben-Hassine 2018](#)

[Nani Jansen Reventlow, Digital rights are \\*all\\* human rights, not just civil and political, 2019](#)