Using social media in CBP - Chapter 8

Connecting Social Media to Offline Protection Activities

Introduction

This chapter relates to the links between Social Media activities and UNHCR actions to deliver protection and assistance. It describes how to integrate protection information collected on Social Media with existing UNHCR data management systems, referral mechanisms and Case Management.

1. Online and Offline

Under the UNHCR, UNHCR Policy on Age, Gender and Diversity, 2018, women, men, girls and boys of diverse backgrounds need to be able to engage meaningfully and be consulted on protection, assistance and solutions. This means that in their operations, UNHCR and partners choose different kinds of participation, making them accessible to all groups in a community. At-risk groups, such as minorities, people with disabilities and people with diverse sexual orientations and gender identities, as well as under-represented groups such as adolescents, youth and older people, must all be included.

On Social Media, giving a voice to all members of a community with a single tool is almost impossible. Many people worldwide still do not have access to stable and continuous internet or mobile devices. And each sector of the population will likely have different preferred Social Media platforms, if any.

To identify and incorporate the priorities and capacities of Persons of Concern into the development of programs, all the while minimizing the risk of excluding them on Social Media, we need to consider two factors:

1. Social Media content and activities need to be well targeted. The situation analysis in Chapter 1 is fundamental for this process;
2. Online protection activities have most impact when they are integrated and interconnected with those offline.

This means that on Social Media, participatory processes will be essential to establish community ownership of programs and allow monitoring and course corrections by the communities themselves. This also highlights the need to connect protection concerns, AGD analysis, digital access and users' mapping in order to design communication strategies that target all sectors of the population.

To be accountable to affected people, UNHCR and partners need to strengthen the links between online and offline communities. These tips may help you make that integration:

- **Use your community mapping:** The Situation Analysis will be the basis of your integration system. There you will find sectors of the population who are both online and offline, and communities that are either one or the other;

- **Focus on protection concerns:** When you or your partners decide (with stakeholders) the protection issues to be addressed with Social Media, and evaluate the associated risks, you can find yourself in one of two scenarios:
  - The protection concern is particular to the online/Social Media world (e.g. scams aimed at selling fake relocation papers to refugees);
  - The protection concern is also found in the offline world (e.g. xenophobic attacks against certain Persons of Concern).

  Both these scenarios require UNHCR and partners to work offline and online simultaneously. Even if you are targeting a protection issue only found on Social Media, you need to be sure that people not yet using SM, or who may hear what can be found on SM, have a basic knowledge of the issue and how to protect themselves and warn others;

- **Think complementary:** If the issue crops up both online and offline, start with what you already have but don't simply repeat online what you are doing offline. If offline activities are being implemented on the ground, for example training for community leaders on peaceful coexistence, you can create complementary activities online. In this example, you might: create community pages to connect host communities and PoCs; engage Social Media influencers locally to discuss the subject on their channels and invite youth into the conversation; conduct an online advocacy campaign using videos and online challenges;

- **Assess, monitor, test and reiterate:** Finding correlations between online and offline information can be difficult. UNHCR and partners cannot assume that information is flowing to offline communities via Social Media. Make sure you have ways to monitor offline effects of online activities and vice-versa. For example, you could add a line to a clinic form, asking people where they heard of a service, to see if they found the information online. Social Media Analytics will also help to understand who is using the information, and how.

2. Referrals

Given the inherent risk of Social Media, it is strongly advised never to use these channels as a means for individual case referrals or case management, or for referrals involving personal data. However, PoCs will often share important and sensitive information with UNHCR via Social Media, both publicly and privately. So it is essential for UNHCR to have effective confidential referral systems for Social Media content, involving internal and external partners who bridge gaps in protection and service delivery.

If you think Social Media will be used for individual case referrals, it is imperative the data controller conducts a DPIA on the SM platform as a tool for case referrals, and all principles in the UNHCR Data Protection Policy (DPP) must be complied with. Referrals may come internally, externally or directly from persons of poncern (self-referral). The most responsive procedures normally consider referrals from all three sources.

While internal referrals occur through UNHCR staff, external referrals usually come from Implementing Partners, other NGOs involved in protection, and government agencies. External referrals help us to identify problems and expand access to protection services.

Important

Informed Consentis the voluntary agreement of an individual who has the capacity to give consent, and who exercises free and informed choice. In all circumstances, including on Social Media, consent should be sought from PoCs prior to referring them to another agency or unit. To be legally valid, consent to handle personal data must be informed, specific and freely given.110 Consent is the most frequently used and preferred legal basis for personal data processing. However, given the nature of humanitarian emergencies PoCs, organizations may not be in a position to rely on consent for personal data processing.

According to the UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR, 2015, when when consent cannot be validly obtained, personal data may still be processed if it is in the vital interest of the data subject, i.e. when the subject's life, security, integrity, health or dignity may depend on it.[111] Whether consent is appropriate depends on a thorough understanding of the situation. Fairness and respect for the rights of individuals require UNHCR to obtain consent whenever the situation allows an informed individual to exercise his/her choice freely.

For Informed Consent, protection officers managing the Social Media engagement must ensure that PoCs fully understand the services and options available (i.e. the Case Management process). They must understand the benefits and risks of receiving services; what information will be collected and by whom, how it will be used and with whom it will be shared; and the limits of confidentiality. UNHCR staff should communicate in a friendly and comprehensible manner and encourage PoCs to ask questions that will help them make decisions regarding their situation.

See more on Informed Consent in the United Nations Protocol on the Provision of Assistance to Victims of Sexual Exploitation and Abuse, December 2019.

In case you are directly approached on Social Media by an individual requesting to be referred:

Weigh the risks of engaging and not engaging with this person on Social Media, and seek other secure means of contact if possible and necessary;

If the decision is to engage, protection staff should introduce themselves and explain their role. Staff should aim to move the conversation to a UNHCR secure channel as soon as feasible;

110 You will find the full definition in the DPP 1.4 and DPG 3.2

111 "Best Interest" refers to the principle set out in Article 3 (1) of the Convention on the Rights of the Child and can be used to justify the processing of children's personal data. For UNHCR, this would require the proper conduct of a Best Interest Procedure (see below: seeking consent/assent from children).

Consent (oral or written) should be sought before making the referral;

To obtain consent, share the identity of the staff collecting the information and their role. Give your contact information and details of the service options available and the provider(s) to whom the person will be referred. Let him or her know the next steps. Explain confidentiality and how their data will be stored, used and shared (if this is the case) by the organizations handling it. Advise the person that at any time they can withdraw their consent and cancel the referral, or request that their personal information be corrected, and/or destroyed. Information about these processes and rights should be communicated clearly, using non-technical language;

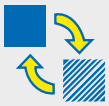
If consent is given - and before any information is collected - technical and/or organizational measures for data protection and data security must be in place to ensure the safe storage and transfer/sharing of information from UNHCR to the service provider. Refer to the UNHCR Data Protection Policy and the Data Protection Guidance for more information on the processing and transfer of personal data of PoCs;

If consent is given, only basic information should be noted down to help the individual access the services he/she requests. Work on a strict “need to know” basis, i.e. only take information that is relevant to providing the specific service requested. In view of the data security concern surrounding Social Media, protection personnel should minimize the collection of personal data to what is strictly necessary for referral. If sensitive personal data is needed, staff should redirect the person to a safer channel, if possible;

Only ask and share the minimum information necessary for the referral e.g first name, contact number and best time to call. And only do it once you have established a secure communication channel;

Depending on the request of the person being referred:

1 Provide the individual with the name and contact details of the service provider (which is not considered a referral) or;
2 Make contact for the individual with the relevant agency/organization through a secure official referral channel.



Tell the person that if they face any problem accessing the service(s) they can come back to referring agency staff or volunteers. If the individual says they are unable to access a specific service, try to provide information on alternative nearby services;

If an individual does not consent, or does not ask you to contact the service providers, refrain from collecting personal data and limit your help to giving information on where to find services and sharing any hotline numbers.

If referrals are done on Social Media, bear in mind the following:

Most Social Media platforms allow you to talk to a user via private conversation (Facebook Messenger, Direct Messages on Twitter, etc.). These “private” channels are not encrypted and should never be used to exchange sensitive information. But you can use them to direct a conversation to a secure channel, e.g. by giving a phone number or email address. Types of data that are ‘sensitive’ in your operational context should be defined as part of the Social Media presence/engagement strategy, bearing in mind UNHCR’s Data Protection Policy;

If you see a lot of people using your Social Media channel to give you private information or information you will refer to NGOs or partners anyway, consider creating a FAQ entry or pinning a post to your Social Media page to direct them to the right channels in the first place;

If your Social Media channel is embedded in an inter-agency mechanism or managed jointly with partners, designate a focal point in each partner organization to have an admin account. In this way you will minimize the copying and sharing of information about referrals on multiple channels;

Make clear your referral pathways on Social Media, even if the conversation is continued offline. People want to know the process, so if you refer them to other pages, accounts or systems, make sure they understand why.

Referrals to Confidential Channels

Very often, and despite clear advice to the contrary, people use Social Media to disclose sensitive information about themselves or others. In Chapter 4, we touched on what to do if someone posts private information publicly on your Social Media channel. To summarize: contact the person immediately, delete the information and engage him or her on a secure channel to discuss their situation.

For private and/or sensitive information, consider the following factors that may differ from offline channels:

1. Protection officers should be available on speed dial for cases that may need an immediate response. You may be in a situation where a Person of Concern can only use Social Media, perhaps for a limited time. In such cases, fast and tested internal referral mechanisms are essential;

2. If someone reports SEA, refer it immediately to the relevant body within the organization. Provide the complainant with a secure channel to communicate;

3. Make sure all admins know the different referral pathways and can explain them clearly in the relevant languages;

4. Always have a pinned post or FAQ with full information on how to make different requests. Who should you contact, when and how?

Interacting with minors online

The explosion of information online has created unprecedented opportunities for children and young people to communicate. But internet access and mobile technology also pose threats to children's safety, both online and offline.

When it comes to protecting children online, we must strike a balance between their rights to information and free expression and their right to safety. Measures to protect them should be targeted and not unduly restrictive, either for the child or other users. In some cases, organizations and companies are starting to promote digital citizenship for children and developing products and platforms that facilitate their positive use of ICTs.

UNICEF developed five key areas for protecting and promoting children's rights online:

1. Integrating child rights considerations into all appropriate corporate policies and management processes;
2. Developing standard processes to handle child sexual abuse material;
3. Creating a safer and age-appropriate online environment;
4. Educating children, parents and teachers about children's safety and their responsible use of ICTs;
5. Promoting digital technology to increase civic engagement.

For more on this topic see UNICEF & GovLab, Responsible Data for Children (RD4C), 2019, and UNICEF, Procedure for Ethical Standards in Research, Evaluation, Data Collection and Analysis, 2015.

3 Connecting Social Media to Case Management

As we have said, PoCs should be warned against sharing personal information on Social Media but if they have done so, damage can be limited and they can be directed to more secure channels.

Information shared via Social Media is hard to verify and can be easy to dismiss as 'fake' or 'uncorroborated'. Nonetheless, if a PoC does reach out to UNHCR via Social Media with information pertinent to their case, it is important this information is appropriately recorded (just like information shared with UNHCR in the offline world).

UNHCR's "Population Registration and Identity Management EcoSystem" (PRIMES) includes UNHCR's digital tools for registration, identity management and case management of refugees (such as proGres v4, RApp and BIMS). Information shared by PoCs via Social Media can be – where appropriate – recorded; for example under the 'add communication' function on ProGres.

Information recorded in the personal/case files of individuals can help to track rights violations, including hate speech, gender-based violence, bullying, intimidation and scams. This will help UNHCR and partners provide the appropriate/tailored protection response.

We can close the loop between UNHCR's Social Media presence and Case Management by making sure PoCs know the proper channels to use to transmit personal information and discuss their cases. We can also work with communities to raise awareness on the possible risks of sharing certain types of information on Social media.

Important

In exceptional circumstances, UNHCR may still need to process the personal data of PoCs in urgent need, despite the lack of secure channels . The privacy and data protection risks need to be balanced against other possibly imminent risks. In such cases, UNHCR staff should tell PoCs the purpose of processing personal data and the accompanying risks of the communications means being used. Restrict collection and processing of personal data to what is absolutely necessary and balance it against the risk of the means used, and bring the issue to the attention of the Data Controller and Data Protection Focal Point. Remember: while processing personal data may only be carried out on a legitimate basis and in a fair and transparent way, including by explicit and informed consent, UNHCR can still process it on one of the following grounds:
(i) With the consent of the data subject;
(ii) In the vital or best interests of the data subject;
(iii) To enable UNHCR to carry out its mandate;
(iv) Beyond UNHCR's mandate, to ensure the safety and security of Persons of Concern or other individuals

See more on: UNHCR, Guidance on the Protection of Personal Data of People of Concern to UNHCR, 2018

Digital Rights Violations

All digital rights (access to information, freedom of expression, freedom of association etc.), are essentially human rights in the internet era. They are based on and protected under international human rights instruments, particularly the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), as well as regional instruments such as the African Union's African Charter on Human and Peoples' Rights.

Criminals are increasingly using Social Media to target vulnerable people with false promises. Examples include the use of Social Media to trick refugees into paying for relocation; Social Media being used by traffickers to influence migrants' decisions and Social Media used to identify, track or even meet minors in person.

This problem is growing in humanitarian situations. Our response focuses on prevention, using offline mass communication, face-to-face communication and consistent messaging on UNHCR channels.

Issues of criminality can be addressed directly on Social Media, which can be used to identify, track and monitor specific protection risks. Below are some examples of how Social Media can tackle possible violations of PoCs' human rights online:

- Most platforms have a function that allows you to report a page or account. If you see any message online that you suspect may be targeting PoCs for scams, you can immediately report it to the platform. Usually, such behaviors are investigated and sanctioned by the platforms themselves as a breach of community guidelines or user agreements;
- Always engage with people who may be sharing false information or scams and explain to them the correct procedures/systems;
- If you believe a Social Media account or page is being used to harm certain people or groups, you should immediately discuss it with protection colleagues and, if necessary, report it to local authorities and the Social Media platform. This is why it is important to ensure individual online risks are documented. Risk in the offline world would be documented and used in Case Management, and the same applies online;
- Discuss with your team what measures you can take to respond to specific posts or address specific risks;
- If you have the resources to sustain it, you may offer PoCs using your site the option to use your expertise to verify information. For example, you can set up a rumor tracking system for online information;[112]
- If you see a lot of users asking similar questions or being confused about the same issue, do not dismiss it. Find out if someone is misleading them. Always ask users where and from whom they have taken "wrong or false" information;[113]
- Make sure you have structures and monitoring systems for your Social Media interactions with PoCs to prevent any misrepresentation or abuse. In rare cases, staff/partners/volunteers may misrepresent themselves under UNHCR's brand, or abuse power using Social Media interactions on behalf of UNHCR to take advantage of a vulnerable person. To prevent this, make sure all staff are trained periodically on the UNHCR Code of Conduct, as well as relevant policies and guidelines.

112 See more on Rumour Tracking in Chapter 6.

113 See UNHCR, 10 Tips to Minimize the Sharing of Misinformation via Social Media Channels, Risk Communication and Community Engagement (RCCE) -COVID 19, March 2020

Connecting offline and online protection activities can maximize the use of resources and the outcomes of both activities. Even in contexts where the offline and online population differs considerably, there are often connections between the two spheres. Understanding these links will help you create online/offline strategies that reinforce each other.

The following suggestions may help you to budget for integrated systems:

- Involve IMOs or IM focal points from the outset: As data specialists, they will be able to help design, implement and review the data elements of your Social Media project. They can also assist in the management of sensitive data (in line with responsible data approaches) and in complying with the Data Protection Policy;
- Map your offline and online activities, and find ways in which the same resource can support both – for example, by engaging outreach volunteers on and offline;
- Invest in educating and promoting safety online;
- Make sure that a rise in PoCs requesting individual case support via Social Media is not linked to a lack of other channels, or people experiencing difficulties with them. If that is the case, you may have to invest in those offline approaches rather than augmenting your Social Media presence;
- From the outset, create strong connections between your on-the-ground protection staff and partners and your Social Media management, so they know what information is flowing and how. This will save you from spending extra time and resources creating these ties when you need them.

Do's	Don'ts
DO make sure all staff knows the referral pathways and how to use them.	**DO NOT** delete messages containing private or sensitive information without contacting the sender and explaining why you removed them.
DO train staff and create monitoring systems for PSEA and child protection, as Social Media is often used by minors.	**DO NOT** assume that just because your page is not intended for minors, they will not access it. The usual safeguarding systems you use offline need to be set up online too.
DO connect with other UNHCR offices in your region or beyond, who may have similar Social Media projects or developed integrated data analysis platforms, before you think about creating your own tool.	**DO NOT** create a bespoke platform. This should be a last resort, only if there is no alternative, and done with HQ to ensure inter-operability with existing systems.
DO connect Social Media projects with offline advocacy, outreach and feedback mechanisms as much as possible.	**DO NOT** assume that Social Media automatically means collecting personal data. In fact you can use SM for protection without collecting any personal data.
DO create workflows and SOPS to connect IMOs with protection staff, so they know what information to exchange, in what situations and how.	**DO NOT** create organizational silos in your Social Media activities and don't restrict SM data management to IMOs.

Check List

- [ ] Have you involved a multi-functional team in discussing internal and external referrals for Social Media content?
- [ ] Do you have SOPs for responding to children or minors online?
- [ ] Have you prepared child-friendly guidelines, spelling out specific risks or scams to which children are vulnerable?
- [ ] Have you prepared a clear and translated set of guidelines for PoCs using Social Media to make them aware of risks and scams?
- [ ] Do you have specific SOPs for Social Media content and/or appropriate systems to handle sensitive communications and referrals?
- [ ] Have you ensured that your Social Media project is connected to UNHCR's protection response, including Referrals and Case Management?

Case Studies

On-Ramps, Intersections and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking, 2018

UNHCR Innovation, Teaching a 'Robot' to Detect Xenophobia Online, 2017

UNHCR Innovation, Chatbots in humanitarian settings: Revolutionary, a fad or something in-between? 2018

UNHCR Jordan, History of the Helpline, 2017

USAID et all, Bridging Real-Time Data and Adaptive Management: Ten Lessons for Policy Makers and Practitioners

Social Media and Forced Displacement: Big Data Analytics & Machine-Learning, White Paper, 2017