Annex 8

Introduction to information and protection training

Acknowledgements

These guidelines are made possible by the generous support of the Bureau of Humanitarian Affairs (BHA) through the United States Agency for International Development (USAID). Internews would like to extend their appreciation to all those who contributed to the guidelines "Information and risks: a protection approach to information ecosystems".

Internews guidelines development and writing team: Stijn Aelbers, Emily Cowlrick, Floriane Echegut, Lea Krivchenia, Haley McCoin, Irene Scott.

Project Advisory Group and peer reviewers: Nadia Akmoun (IOM), Raphael Bacot (REACH), Adrienne Brooks (Mercy Corps), Stuart Campo (OCHA), Victoria Dangond Peralta (Internews), Marina Di Lauro (Oxfam), Katie Drew (GPC), Marie Dozin (GPC), Tiffany Easthom (Nonviolent Peaceforce), Giovanna Federici (NRC), Andre Heller (IRC), Séverine Lacroix (IOM), Anahi Lacucci (UNHCR), Francesco Michele (GPC), Briana Orr (IRC), Nathaniel Raymond (Yale University), Joelle Rizk (ICRC), Fausto Spiga (REACH), Mark Silverman (ICRC), Kathrine Starup (DRC), Craig Twitt (Internews), John Warnes (UNHCR).

Design and illustrations: Corneliu Comendant, Emily Cowlrick, Floriane Echegut, Julia Huang, Ganaëlle Tilly

These resources have been created as part of the Community Voices for Better Protection (CVBP) project. This project aims to understand the risks associated with information in humanitarian contexts from the perspective of humanitarian field workers, specialist protection agencies and media and other information providers. Using field work conducted in 2022-23 in three locations – Iraq, Mali and Philippines – these resources work to address a gap in the understanding of, and response to risk and information.

For feedback or suggestions for the improvement of these guidelines, please contact the Internews Humanitarian Team through info@internews.org

Annex 8: Introduction to information and protection training

This training curriculum and exercises aim to support humanitarian and media actors in building the capacity of their team prior undertaking a protection analysis of the information ecosystem, or simply to foster understanding of risks related to information.

This is an introductory training course that targets staff with little or no expertise in information and/or protection and should be used together with the Guideline Modules and Annexes.

Curriculum and learning objectives

Learning objectives	Corresponding Exercise	Approximate duration	Resources
Information			
Information terminology: Participants will understand the key words and concepts required to understand information needs and potential barriers to accessing information.	See exercise 1 – Team game	30 minutes	A4 colored paper with words, definitions, and blank (for examples).
Protection			
Protection analysis: Participants will understand protection analysis (namely activities to identify threats, vulnerable people, perpetrators, and responsibilities and roles for taking action) and how to apply it to the local context and Internews' work.	See exercise 2 - Role play activity and guided discussions	45 – 60 minutes	Annex 1 – Glossary, Scenarios (provided in exercise 2)
Vulnerability analysis: Participants will understand the factors that make people vulnerable (or less vulnerable) to threats and how to analyze power differences. These skills will help them design projects that are tailored to the needs of the community members based on a multitude of criteria rather than relying on classic selection criteria.	See exercise 3 – 'power walk' / one-step forward exercise, followed by facilitator-led discussion	45 – 60 minutes	Fictional character sheets adapted to the local context, pre-planned identification questions to match characters (guidance provided in exercise 3)
Safe programming			
Safe-programming assessment: Participants will know how to conduct a "do no harm" risk analysis (through the use of a basic template) and how such assessments contribute to protection mainstreaming's four principles.	See exercise 4 – watching video, guided discussion and practice using safe-programming assessment	45 – 60 minutes	Global Protection Cluster video, capacity to show video, flipchart, Annex 2 - conducting a safe-programming assessment template
Safe and timely referral: Participants will know how to undertake a service mapping and conduct referrals in a safe and timely manner.	See exercise 5 – group work and presenting back	Duration: 30-45 minutes	Power point, project, 'Do- and don't' example sheets (provided in exercise 5).

Trainer(s) profile:

Each topic in this training is introductory level, and covers three areas of expertise: information, protection, and safe programming. Though it is introductory, it is recommended that the Trainer specializes in least one of these topics. Additionally, the Trainer should be thoroughly familiar with the content of the guidelines to fill potential knowledge and contextual examples gaps for the other topics. Module 1 will support introducing the training, Module 2 can support training on safe programming, and Module 3 on protection analysis. The Annexes will also be helpful, especially the Glossary (Annex 1) and the Safe Programming Assessment Template (Annex 2). For a group of training participants mainly constituted of journalists, Module 4 will provide additional information to support tailoring this training to that type of group.

Exercise I: Information terminology

Understanding the necessary terminology around information needs, in order to undertake an information-related protection analysis.

Exercise format: Team game where each team moves from one table to another to pair words with definitions. When moving to the next table with a new group of words, the group reviews the pairing made by the previous team. After all pairings are verified and explained, participants start a new round where each team is tasked with providing examples for each word/ definition combination. Teams then discuss to verify examples and strengthen participants' understanding of information terminology.

Preparation: A4 colored paper with words, definitions, and blank (for examples).

Duration: 30 minutes

INFORMATION TERMINOLOGY	
Disinformation	False information which is deliberately intended to mislead
Misinformation	False or inaccurate information, spread accidentally or without the deliberate intention to mislead or cause harm
Rumors	Unverified information passed from person to person (can be true or false)
Fake news	Fabricated information that mimics news media content
Source	The person, organization, or entity that produces/creates information
Channel	The platform/person that someone uses to obtain information
Literacy	The ability to read and write
Information literacy	The ability to understand/analyze information and the validity of different information sources
Digital literacy	The ability to safely find, analyze, and communicate information through digital platforms

Exercise 2: Protection analysis

Outlines the key definitions and concepts used in protection and contextualizes protection risks around access to information and local contexts.

Exercise format: Role play activity followed by guided discussions to introduce participants to the concept of protection risks, technical terminology, and steps needed to conduct a protection analysis. The facilitator will use scenarios to explain the components of the protection risk equation (threat, vulnerability, and capacity). For definitions of protection terminology, including the protection risk equation, see *Annex 1 – Glossary*.

Duration: 45-60 minutes

Preparation: Use the two scenarios provided below for role play. Each scenario includes elements of:

1. the three protection threat categories (coercion, deprivation, and violence)
2. vulnerability and capacity characteristics, and
3. identifying the perpetrator.

Guiding discussion for running the scenario:

- You can adapt the scenarios, but one scenario should focus on offline risks and one on online risks.
- Use the protection risk equation in the Annex 1 – Glossary to guide discussion.
- Two participants can perform one role play exercise twice (once in English and once in local language as needed).
- Then, the group discusses the story piece by piece and identifies the different threats, vulnerabilities, and capacities.
- It may be useful to go through several examples so participants can grasp the multitude of threats that could exist including barriers to access, extortion, trafficking, abuse, etc.
- Repeat the same process with the second role play exercise.
- Once all threats, vulnerabilities, and capacities are identified, the protection risk equation can be introduced and examples from the discussion can be used to identify how government, media, relief organizations, and community networks could work together to reduce threats and vulnerabilities while increasing capacities, to reduce the identified protection risk.
- The discussion following the role play will address the question: "what would your organization do to help in this situation?".

Scenario on offline risk example

Woman: Hello, I would like to buy a SIM card. My plan does not work here.

Man: Good afternoon, I will need your local identity (ID) card or passport to register the SIM card.

Woman: I do not have a local ID or passport, we lost everything when we came here. Another vendor refused to sell me a SIM card because I am a woman, another wanted extra money, now this. What is this new rule?

Man: I won't give you a SIM card, that is the rule. If you don't like the rules, you can leave.

Woman: This cannot be true! You have to help me, please?

Man: Are you calling me a liar?! Get out of my shop woman, or else I'll beat you.

Woman: I am sorry, please let me buy a SIM card, it is my only way to contact my family and I need internet. I don't understand anything on the TV or radio here, I need to access news online in my language.

Man: Well, let's see, maybe if you come to the back of my shop, and are very nice to me, I'll find you a SIM card.

Scenario on online risk example

Man: Oh, my dear friend, I am really worried and I need your help.

Woman: What happened? Everyone is worried with the storm coming, why are you not in a shelter with your family?

Man: This is the problem. Families in my neighborhood did not receive any information, we did not know what to do. The radio broadcast said not to move until we get direction from the Government Crisis Team, but we never got any for people living in camps.

Woman: It's okay, I don't believe the news so I am staying too. You just need to prepare the house and your family will be fine, it's just a light shower.

Man: My family will not be fine -- my children were taken by a woman! I found this group on Facebook that had information on shelters, and a woman offered to host all of us. She was so kind and offered to bring the children first, to make sure my wife and I had time to prepare the house for the storm. We and another family dropped off the kids in the morning. When we went back this afternoon to join them, no one was there!

Woman: That is horrible, you must call the police!

The man receives a notification on his phone...

Exercise 3: Vulnerability analysis

How to holistically assess factors that influence vulnerability, capacity and power dynamics

Exercise format: A ‘power walk’ followed by a facilitator-led discussion with participants to understand vulnerability, capacity, and power dynamics, and their impact on project design (by reducing vulnerability or increasing capacity of the community and key stakeholders, or identifying advocacy targets).

Participants need to line up with a clear space in front of them. Each is assigned a fictional character. The facilitator reads a series of questions that highlight power dynamics and different factors which influence vulnerability and capacity of an individual. For each example where a participant feels their character possesses the necessary characteristic to benefit from the example given, the participant takes one step forward. After the 10-12 questions are done, each participant discloses their fictional identity and discussions take place among the group to validate or correct the end positions of participants. In this stage, participants can discuss a multitude of elements that influence people’s access to information, selection criteria for beneficiaries, advocacy targets, and elements of activity design that address vulnerability/capacity.

Preparation:

- fictional character sheets adapted to the local context
- questions to enable the identification of vulnerability and capacity elements, adapted slightly for the local context and adapted characters as needed

Duration: 45–60 mins

Questions :

1. Can you write and read?
2. Do you speak the same language as the main TV channel, radio, and newspaper that publishes news?
3. Can you easily access information in your preferred language?
4. Do you have access to a radio or phone to listen to the news and other programs?
5. Can you charge your radio or phone at home?
6. Can you rely on family, friends, non-government organizations (NGOs), or your work to get information you need?
7. Do you have private access to the internet?
8. Do you know how to use social media sites like Facebook and WhatsApp?
9. Do you have a different password for each device (namely for your phone, laptop, and tablet if you have multiple devices) and each application (for instance do you have a different password for Facebook, WhatsApp, email account, banking apps, etc.)?
10. Do you always log out of your account when using a public device (including laptops, phones, or tablets used by other people?
11. Do you verify or check information before sharing it with others, or before acting upon it?
12. Do you hold influence in the community? (for example, do you have access to a forum to share your views with large amounts of people regularly)

Character 1:

You are a woman in her sixties who lives in an IDP camp with little to no social or economic power. You never learned to write or read. You love spending time with your neighbor to listen to the radio with her, but it is hard to understand because you come from a place that speaks a different language. You have a smartphone but use it only to make calls, all those online things are too complicated!

Character 2:

You are a blind woman who teaches history at the university. You can write and read in braille (a language used by blind people) and have easy access to audio news from your favorite newspaper which publishes in your preferred language. You are on social media, but your Twitter account was suspended because you shared a post from a friend that was considered fake news – you forgot to verify information before sharing it!

Character 3:

You are a teashop owner in the main market of the city. The TV or radio are always on in your teashop, and you love discussing the news with your customers. Sometimes you even argue with them because some news seems fake, and it is hard to determinate what is **really** happening! You created a private group on WhatsApp to share information published by local and international newspapers with your friends – only verified information is shared on the group.

Character 4:

You are an internally displaced girl who works in a factory. You dropped out of technical college after two years. You find it hard to communicate with people from the host community due to language barriers. However, you get all your news in your language from your smartphone. Your Facebook account was hacked a few times, maybe because you never log out of public computers!

Character 5:

You are an illiterate old man living in a refugee camp. Recently your relatives went back to where they are from. You don't understand local news due to language barriers, but you are communicating with national and international NGOs for information. You can't decide whether to go back to where you are from or not because you are confused and don't have enough information.

Character 6:

You are a young woman who borrows her brother's phone to get information online. It's hard because you have to use his account every time. You need to use his Facebook, but everything is written in <*insert relevant language*>, and you would prefer to get information in <*insert relevant language*>. Your brother only agreed to let you use his phone because you can charge it at the local women's association – electricity is a problem at the moment, but the association has a generator.

Character 7:

You are a man who became deaf after a large explosion damaged your hearing. You find it hard to understand information because you cannot read, and you cannot listen to the radio like before. An organization helped you get a phone and internet credit, but you don't know where to find the information you need online. Anyway, the phone is almost always turned off because there is no electricity to charge it. As soon as you switch it on, you receive lots of calls because you shared your number online to get information on services for people with a disability. However, you cannot hear people so there is no point in them calling you!

Character 8:

You are a grandmother that wants to stay connected to new technologies. You have a phone and use it to post news on Facebook and Instagram. Your granddaughter keeps calling to ask you to remove some of your posts because they include fake news. You thought since your friend shared it, it must be true. The problem is that you speak <*insert relevant first language here*>, but all local news is in <*insert relevant second language here*>. The internet is the only place where you find information you need in <*insert relevant first language here*>.

Character 9:

You are the head of a famous local radio station and are very proud of the content the station broadcasts. Lately you saw online complaints from several people who live in the city and speak a minority language because your shows use the most common local language and they don't understand the broadcasts. They would like the radio to include news about their community too. You tried to delete their complaints on the radio's Facebook page, but it created more problems.

Character 10:

You are a journalist who works on identifying fake news. You love going on the internet to see the rumors and misinformation that circulate on Twitter and Facebook. You created a private group on Facebook that lists all the fake news circulating in your community and provides verified information and alternative sources to help people compare information. You are trying to convince a local newspaper to write an article on this topic, but you don't speak the language used by the newspaper so they would prefer to work with someone else.

Exercise 4: Safe-programming assessment

Introduction to protection mainstreaming principles and direct application through a "do no harm" risk analysis of existing or upcoming project/activities.

Exercise format: As a group, watch this video on Protection Mainstreaming from the Global Protection Cluster (GPC).

Video link:

Following that, talk through the mainstreaming principles as a group, with participants providing at least one practical example from their work for each principle.

Then, present each participant with the template for conducting a safe-programming assessment (template in Annex 2). Watch the video again.

The group discusses:

- Protection risks present in an existing or upcoming project/activity within their work (risks can be assessed based on those posed to the community, organizational / media outlet staff, local partners, and for the organization/media outlet's brand).
- Mitigation strategies for those risks can be discussed
- Mitigation roles and responsibilities among teams and partners involved

Preparation: set up projector / monitor to view the GPC video (be sure to verify the audio and subtitles), set up a flipchart with a template for the protection risk analysis

Duration: 45-60 mins

Exercise 5: Safe and timely referral

Introduction or refresher on service mapping, and key elements for safe and timely referrals.

Exercise format: An exercise on “referral do’s and don’ts” where participants review a list of actions and decide together whether those are good or bad practices. This can be done in groups depending on the number of participants. A discussion takes place during the correction phase where remaining questions can be answered. A Flipchart or PPT slide can be displayed during the correction and discussion phase to

- review key principles for safe and timely referral (namely confidentiality, informed consent, not raising expectations, etc.)
- introduce and discuss available resources for service mapping, including (when available) the OCHA “ReliefWeb Response” website which offers a dashboard of each cluster and contact details for focal points). The participants should then identify community mechanisms that are safe and available and build trusted relationships with the focal points operating them.

Preparation: ‘Do- and don’t’ examples – to be mixed and then placed by participants on two separate columns on A4 paper (one column for DO, and one for DON’T), set up projector / monitor to view Powerpoint slide showing the principles of safe referrals (one slide – copy of diagram below) and OCHA ReliefWeb Response website (one slide – linked above). If projector and laptop are not available, the slide can be reproduced on a flipchart.

Duration: 30-45 minutes

DO	DON’T
Be prepared. Find out in advance what services and support are available locally.	Pressure the survivor to provide additional information or details.
Make sure you and the person are safe from immediate harm.	Provide counseling.
Treat the information confidentially and listen to the person in a safe and private place.	Record details of the incident or the victim’s personal information.
Respect the survivor's right to make their own decision.	Offer advice or judgments.
Listen to the person without asking questions.	Make false promises or provide false information (or information you are not sure of).
Behave appropriately, taking into account the person’s customs, religion and gender.	Assume that you know what the victim wants or needs. Some actions may put the victim at additional risk of stigma, retaliation or harm.
Limit the number of people who know about the case (refer the case confidentially to the appropriate GBV Focal Point and only with the victim’s informed consent).	Investigate the event prior making a decision on whether to refer or not.

See Annex 8 – PowerPoint presentation for a full-page version of the slide below.

What is a referral?

- A **referral** is the process of directing an individual or a household to another service provider because they require further action to meet an identified need that is beyond the expertise or scope of the current service provider.
- A **self-referral** is the process of an individual making a request for assistance to the needed service provider themselves, either in person, on the phone or through a digital channel.

Guiding principles

RESPECT CONFIDENTIALITY

- By only sharing disclosed information and only allowing access to it after informed consent from the person is obtained.
- By ensuring information is collected, stored and shared in a safe way.
- By only collecting and sharing the minimum information required - on a 'need to know' basis - to allow the service provider to respond to the referral.

OBTAIN INFORMED CONSENT

- By seeking oral, and where possible, written permission directly from the person to proceed with recording their information and by conducting a referral for them.
- By ensuring the person has the capacity, maturity and adequate information to know what they are agreeing to.
- *There are only three exceptions to this rule: where there are indications that a person is planning to take their own life, or planning to harm the safety of others, or where a child is at imminent risk of harm, can you conduct a referral without informed consent. For children, always consider the best interest of the child.*

DO NOT RAISE EXPECTATION

- By clearly explaining the steps of the referral process and the expected time frame to the person, and avoid making promises about the outcome of the referral.

RESPECT CHOICE AND DECISION-MAKING CAPACITY

- By listening in a non-judgmental manner, and accepting the person’s choices and decisions. This is particularly important for survivors of gender-based violence.
- Do not investigate. Let the specialized service providers do this as needed to avoid inadvertent re-traumatization

PRIORITISE THE SAFETY AND SECURITY OF THE PERSON FIRST

- By considering and communicating the risks the person might face when accessing the service or assistance.

What information do you need?

- Service mapping of all locations where you plan to implement
- Referral mechanisms to use, usually developed at Cluster level by each cluster (Gender Based Violence (GBV) + Child Protection (CP)!)

Where to find this information?

- Public services website (always verify)
- Clusters - depending on service needed (Protection Cluster for anything related to immediate risk or response to a threat that already occurred – GBV and CP required specialized protection staff)
- OCHA ReliefWeb website
- Community leaders

Guidelines map: How do I use the *Information and risks: a protection approach to information ecosystems modules and annexes?*

Question:
I run the online page of a local newspaper and I have heard some rumors that violence broke out after an article we wrote prompted very angry comments.

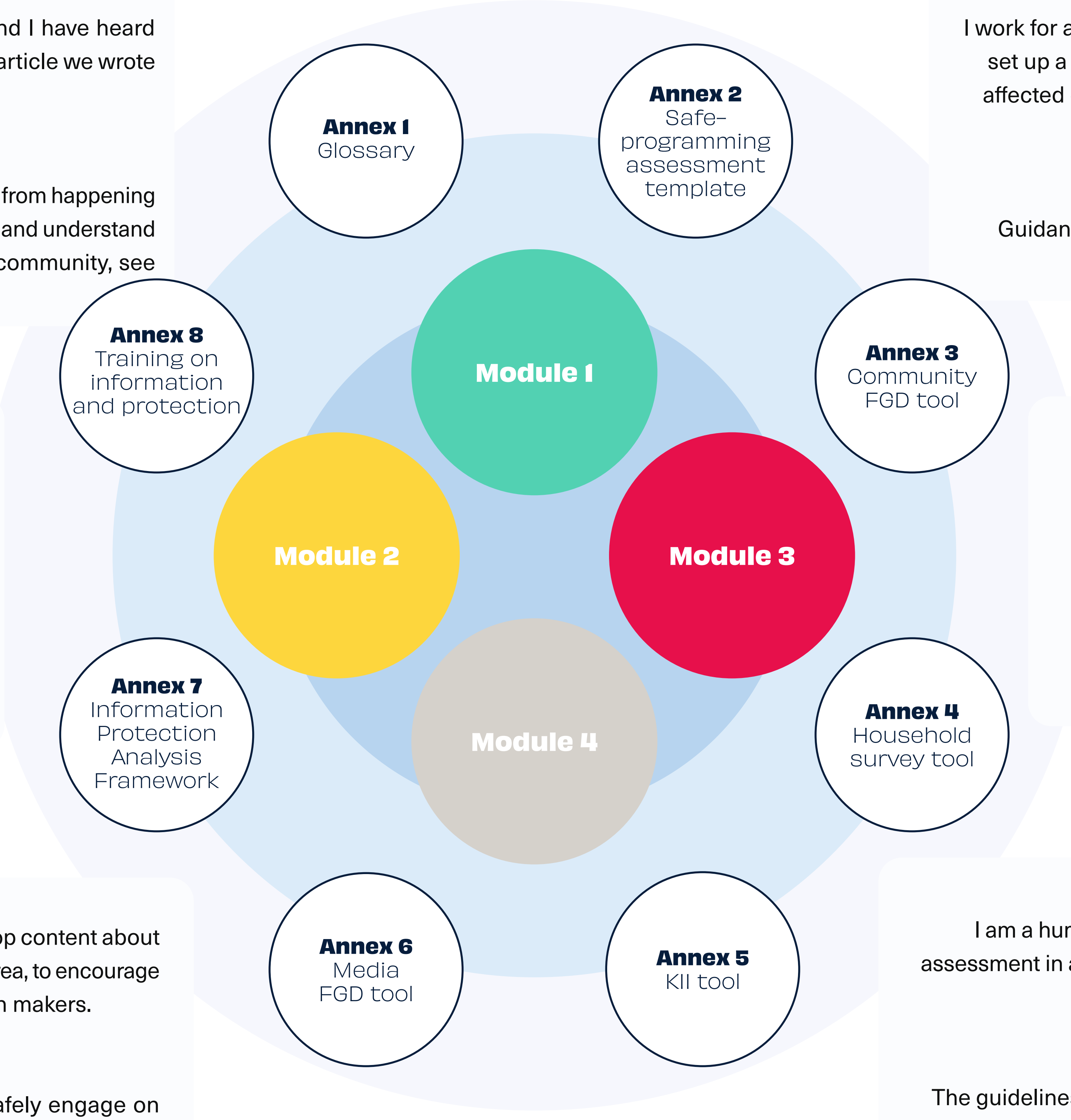
Answer:
To guide work aimed at mitigation and preventing this from happening again, see Modules 2 and 4. To listen to communities and understand more about the issues this article triggered in the community, see Module 3 and associated tools.

Question:
I am a protection actor preparing to undertake analysis to monitor protection trends and inform programming.

Answer:
Module 3 and associated Annexes provides an analytical framework to help you design your tools and collect data, as well as guidance to produce analysis on information-related protection risks.

Question:
I work at a local radio station and want to develop content about the rise of gender-based violence (GBV) in the area, to encourage action amongst regional and national decision makers.

Answer:
The guidelines will provide direction on how to safely engage on sensitive information (Modules 2 and 4) and how to analyze the role of information in reducing or exacerbating GBV in the community (Module 3).



Module 1

Module 2

Module 3

Module 4

Annex 1 Glossary

Annex 2 Safe-programming assessment template

Annex 3 Community FGD tool

Annex 4 Household survey tool

Annex 5 KII tool

Annex 6 Media FGD tool

Annex 7 Information Protection Analysis Framework

Annex 8 Training on information and protection

Question:
I work for an non-government organization and I want to set up a Facebook page to share information with the affected community. How can I make sure it is safe for community members to use?

Answer:
Guidance on setting up safe, meaningful and accessible information channels can be found in Module 2.

Question:
I work for a humanitarian organization and want to review (or if needed, develop) a feedback and complaint mechanism.

Answer:
Module 2 will provide information on safe and meaningfully accessible feedback and complaint mechanisms.

Question:
I am a humanitarian coordinator leading a multi-sectoral assessment in a country that was hit by a humanitarian crisis. How do we engage safely with communities?

Answer:
The guidelines provides guidance on how to safely engage with communities and coordinate with key stakeholders in Module 2. Module 3 provides guidance on how to include information elements in an assessment.