Annex I

Glossary

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 I: Glossary

This Annex aims to guide use of terminology used in Safe, Meaningful and Accurate Information: A Protection Approach to Information Ecosystems guidance and tools. Given this guide seeks to harmonize and utilize terminology from the protection sector and information ecosystem schools of thought, terms have been used specific to these practices and therefore may differ slightly from dictionary terms, and reference specific contextual thinking. If you believe additional terms from the guidance or tools should be added here, or if any terms need clarification, please contact the Internews Humanitarian team.

Information Glossary

Access to information: The ability to create, share, seek and obtain information.

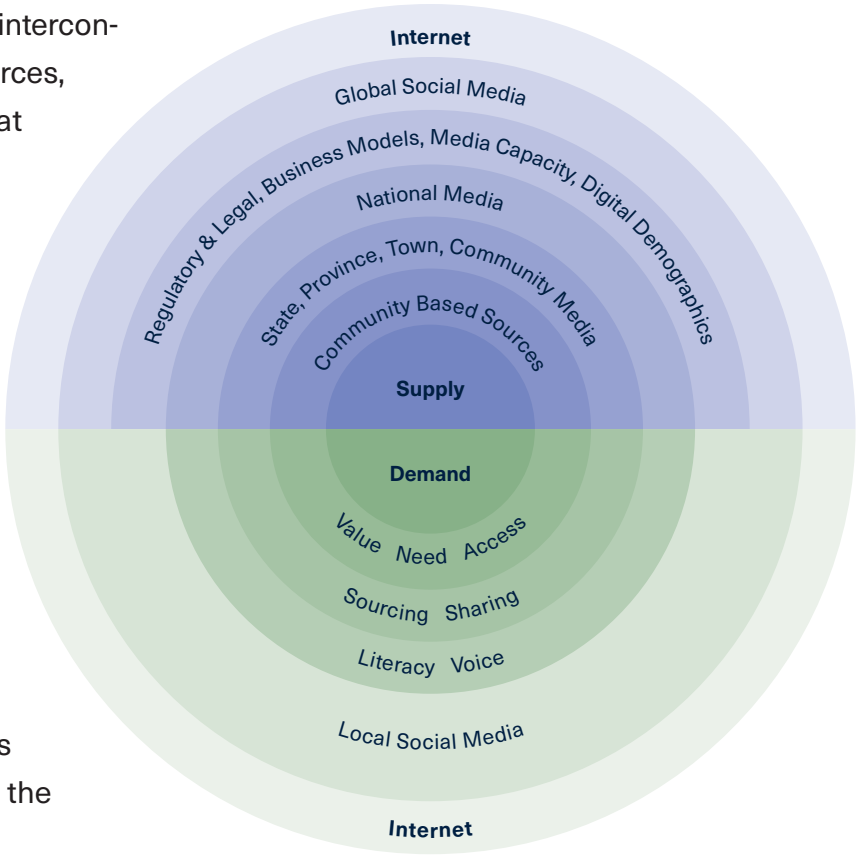
- **Creating information:** Creating information refers to information that is curated to reach an audience beyond the immediate peer of the creator. This can be done by an individual, group, organization or professional content creators such as media outlets. It goes beyond simply sharing raw information, and involves a level of creation, curation or personal input into the form of how the information is presented.
- **Sharing information:** For the purposes of these guidelines 'sharing information' refers to sharing information without further packaging that information in any way.
- **Seeking information:** Seeking information refers to the act of looking for or requesting information (or content) from an information source/s or provider/s (see below for definitions), both online and offline, through any channel and in any form (verbal, written, visual, etc.).
- **Obtaining information:** Obtaining information refers to the act of receiving information (in the form of raw information or curated content) from information sources or providers (see Annex 1 for definitions of these actors), both online and offline, through any channel and in any form (verbal, written, visual, etc.).

Channel and platform: Channels and platforms house or transmit information. These typically refer to technology channels or platforms, such as television, radio and online / digital spaces such as social media platforms or websites.

Digital literacy: Digital literacy is the ability to find, critically evaluate, organize, use, and communicate digital information through digital channels, platforms and sources, with particular awareness for the risks and threats faced when using digital channels, platforms and sources.

Information actor: Individuals or institutions involved in generating, disseminating or influencing information. This can include creating or influencing legal and regulatory environments that relate to information (for example, government), actors doing research in relation to information (academia, activists working on data security, freedom of speech), actors collecting and documenting information (human rights actors, humanitarian agencies, special interest organizations), or actors creating information (see: information providers).

Information ecosystem: The interconnected network of various sources, channels, and platforms that facilitate the creation, dissemination, and consumption of information within a particular community, environment, or context. The ecosystem includes traditional media outlets, social media, websites, individuals, organizations, governments and other entities that contribute to the flow of information and influence how it is accessed and understood by the community or audience.



Information literacy: Information literacy is the ability to find, critically evaluate, organize, use, and communicate information in all its various formats, most notably in situations requiring decision making, problem solving, or the acquisition of knowledge.

Information provider: An information actor (individual or institution) that makes deliberate efforts to make information accessible to an audience beyond their immediate personal network. This term refers to information providers as individuals or groups using public (sometimes online) channels, government institutions, civil society organizations, or media organizations. Information can be provided to the general public or specific target audiences.

Note regarding online posting: Internews makes the distinction between someone from the community posting something online without necessarily trying to inform the wider public (but with potentially a large reach) from someone who makes a deliberate effort to collect and

collate information with the aim to reach an audience. The former is part of the conversation within a community and could serve as a source for primary (online) data collection, while the latter is seen as an information provider

Journalist: A journalist aims to investigate, report, and communicate factual (descriptive and sometimes evaluative) and informative information that is of public interest across various media platforms. Journalists follow a set of norms and rules that hold them accountable to ethical behavior, professional standards and a commitment to rectify mistakes.

Media Worker: A media worker works in a media organization to contribute to the production of news and informative content. This could include roles that are associated with journalists such as editors, camera

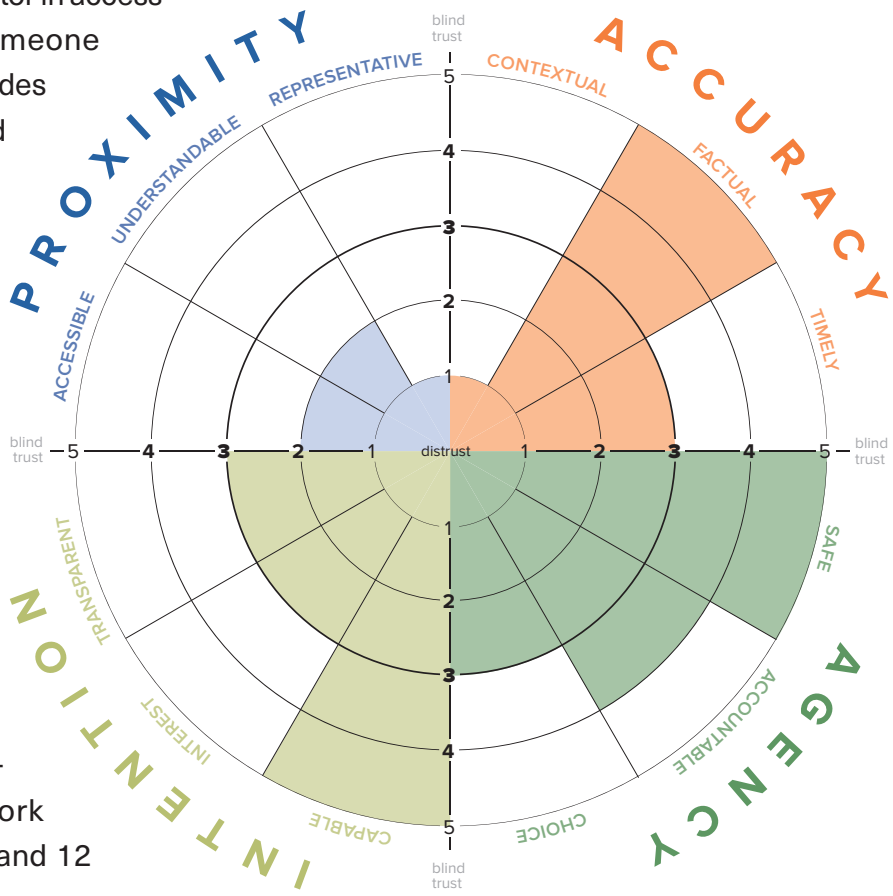
Content Creator: A content creator is an individual who generates various forms of digital content, such as videos, blogs, or social media posts, often for online platforms. Unlike professional journalists, content creators are not bound by journalistic ethics or editorial oversight. Content creators may create content for their own personal channels or, for example, may be contracted to create and share content on behalf of a community, civil society or other organization or group.

Media: professional organisations guided by editorial and ethical standards who use the means of communication, as radio and television, newspapers, magazines, and the internet, to reach or influence people widely.

News: Defined as a selection of information about current events.

Source (of information): Refers to the primary information from individuals or institutions. An information source can be from an information provider, but also refers to information from any individuals or institutions that collects, creates, or collates information. It can include first-hand witnesses, experts, documents and primary data that is used to create information, including social media posts, official documents, data, research studies. When multiple sources are used to create a new overview, analysis or other type of content, this in turn can be considered a new source of information. In this sense, a newspaper article can be an information source, while the news organization that has produced it, is understood as an information provider.

Trust: Trust is a fundamental factor in accessing information. Whether someone trusts an information source guides if they will listen to, act on, and share the information gained from that source. A lack of trust usually leads individuals and communities to not engage with a certain information source, and blind trust can result in lower levels of agency and a higher risk of mis-, dis-, and malinformation. Internews developed the [Trust Analytical Framework] to help contextually define and measure trust in information providers. The Framework consists of four components and 12 sub-components.



Protection Glossary

Capacity: The resources and capabilities that are available to individuals, households, and communities to cope with a threat or to resist or mitigate the impact of a threat. Resources can be material or can be found in the way a community is organized. Capabilities can include specific skill sets or the ability to access certain services or move freely to a safer place.

Protection analysis: A process undertaken to identify protection risks with the aim of informing strategies and responses.

Protection risk: Actual or potential exposure of the affected population to violence, coercion, or deliberate deprivation. The protection risk equation (visual below) is a non-mathematical representation of the three factors that contribute to risk. A Protection risk arises when the threat and the vulnerability (of an individual or a community) are greater than the capacity to prevent, respond, and recover from that specific threat (Global Protection Cluster definition).

Protection risk equation (Global Protection Cluster)

Protection threat: a human activity or product of a human activity that results in violence, coercion, or deliberate deprivation.

- **Violence:** The intentional use of physical force or power, threatened or actual, against one-self, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation.
- **Coercion:** Forcing someone to do something against their will.
- **Deliberate deprivation:** Intentional action to prevent people from accessing the resources, goods, or services they need and have the right to access.

Vulnerability: Certain characteristics or circumstances of an individual or group, or their surrounding physical environment, which diminish ability to anticipate, cope with, resist, or recover from the impact of a threat. People differ in their exposure to a threat depending on their social group, gender, ethnicity, age, and other factors. Vulnerability is not a fixed or static criterion attached to specific categories of people, and no one is born vulnerable.

Information meets Protection Glossary

Information-related threat: A human activity or a product of human activity that finds its root or is sustained by factors in the information ecosystem, and that results in a form of violence, coercion, or deliberate deprivation. Threats can be the perpetrator (agent of the threat) or a policy or an ethnicity norm (source of threat) that is causing harm.

Personally identifiable information (PII): Any information that indicates someone's identity, or which allows someone's identity to be inferred by a reader. Examples would include full names, addresses, aliases or phone numbers.

Information risks: Any risk that is the consequence of the information ecosystem. The actual or potential exposure to the risk is deliberate or not. This includes but is not limited to risks resulting from misinformation, rumors, barriers to access information, lack of information.

- **Misinformation:** False information that is spreading, regardless of whether there is intent to mislead or cause harm.
- **Rumors:** unverified, first-hand community data. This can be unverified, but factually correct, partially correct or incorrect.

Information-related protection risks: This includes actual or potential exposure of the affected population to violence, coercion, or deliberate deprivation where there is a deliberate attempt to use the information ecosystem to harm. This could be denial of access to information or disinformation and should take into account the effect of those risks on other protection risks, as well as on negative coping mechanisms that could increase vulnerability of the affected population to other protection risks.

- **Denial of access to information:** Denial of access to information is established when the freedom to create, share, seek, and obtain information is purposely "impaired in such a manner and to such a degree that it hinders the capacity of the affected communities to enjoy basic rights and fulfil their basic needs" (Global Protection Cluster definition)
- **Disinformation:** Disinformation is defined as the intentional dissemination of false information to cause harm, it "misleads the population and, as a side effect, interferes with the public's right to know and the right of individuals to seek, receive, and impart information" (Global Protection Cluster definition).

Safe and meaningful access to accurate information

- **Safe access to information:** Access to information is safe when a person or group does not face risks while creating, sharing, seeking and obtaining information
- **Meaningful access to information:** Access to information is meaningful when it is accessible to all population groups based on their information needs and preferences including preferred language, literacy level, and preferred approaches.
- **Access to accurate information:** The conditions of 'access to accurate information' comprise when people have the have the tools, capacity, and resources needed to verify and analyze information. This can include digital literacy, informational literacy, and fact-checking knowledge, as well as available related resources from information providers.

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:

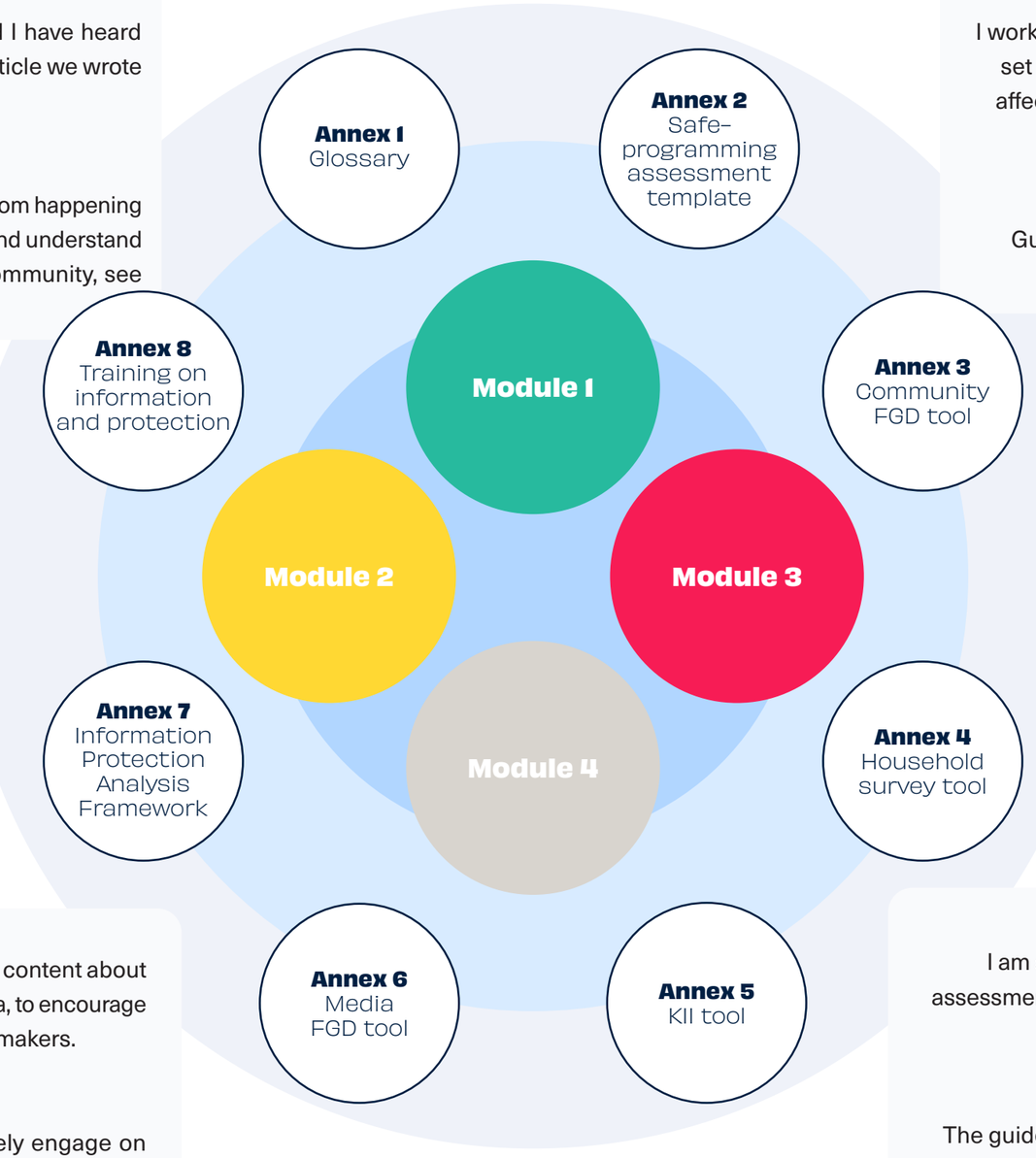
Module 3 and associated Annexes provides an analytical framework to help you design your tools and collect data, as well as guidance to produce analysis on information-related protection risks.

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).



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.