CLEAR Global

United Kingdom Humanitarian Innovation Hub

elrha

UK International Development
Partnership | Progress | Prosperity

How to hold organizations accountable for their use of digital technology

a guide for crisis-affected communities

Created by
CLEAR Global
For United Kingdom Humanitarian Innovation Hub
Wih support from UK International Development

Unit 1

How to use this guide

Unit 1. How to use this guide

This guide is intended to support crisis-affected community members to hold humanitarian organizations accountable for their safe and responsible use of digital technology. This technology may be newly developed digital tools or existing tools combined in new ways. It includes innovations in the early stages of development and more mature and established solutions ready to be implemented at scale. Whatever the case, decisions about how the technology is implemented and used must be responsible, ethical and inclusive.

To help ensure those decisions have the best impact for you as community members, you need information. You need to know how the technology proposed might affect you, what you can expect of the organization proposing it, and how you can put your views or raise concerns. The guide aims to equip you to get the information you need and take action on that basis, either individually or collectively.

The guide is divided into 11 practical units

The guide is composed of 11 units, which can be used separately or in combination. Most units contain a summary of the key points you should know, if you just want the essential information, and a fuller version if you want to know more.

01 How to use this guide
You can refer back to this for a list of all the units and how to use them.

02 Know your digital rights
A summary of your rights relating to the responsible humanitarian use of digital technology. Refer to these to hold organizations to account.

03 How should communities be involved?
What consultation to expect on humanitarian uses of technology, and what decisions are made at each stage.

04 Common risks and how to avoid them
Some of the common risks communities can face when humanitarians use digital technology, and what you and the organization can do to avoid them.

05 What digital risks look like in practice
Short examples of how common risks can arise with digital technology, to help assess potential risks for your community.

06 How to spot unsafe uses of digital technology
A list of 'red flags' you can use to quickly spot when humanitarian use of digital technology is unsafe.

07 What you have a right to know
Questions to ask a humanitarian organization about their plans for digital technology, to understand the risks and opportunities.

08 Information form for holding an organization accountable
You can use this to keep key items of information in one place for community members to refer to.

09 How to report a problem
A step-by-step guide to reporting a problem or making a complaint, with an email or letter template you can use.

10 What does that mean? A digital rights glossary
Brief plain-language explanations of key terms. Terms explained in the glossary are highlighted **like this.**

11 Where's my data? A game for understanding about data privacy
A guide for a game to help people become more aware of what can happen to their data and what that could mean for them.

Please use, adapt and provide feedback on this guide

Every community, every emergency and every organization is different, and one guide can't cover them all. Instead we hope that those who find this guide useful can adapt it to their contexts, including by translating it into the languages of crisis-affected community members. If you do that, please let us know, so others can learn from your experience.

Do you have comments or feedback about this guide? We'd love to hear them. Email us at: info@clearglobal.org

Unit 2

Know your digital rights

- The main principles, standards and laws that humanitarians must apply when using digital technology
- What they mean for the rights of communities where they operate
- Examples of how these rules apply in specific cases
- Your right to make a complaint if an organization doesn't apply the rules

The key things to know about your digital rights

Rules apply to how humanitarian organizations use digital technology. They must:

Not exclude people from services through their use of technology

Assess, monitor and protect against possible risks to community members

Protect users' personal data against misuse and unauthorized access

Provide a channel to report problems and make complaints

It may help you to refer to these these **rules** when discussing risks or problems with the organization or when making a complaint.

Unit 2. Know your digital rights

How to use this information

Humanitarian organizations use digital technology where they think that it will provide communities with better, faster or more efficient support in an emergency. As technology evolves, its potential benefits continue to expand, including the potential to connect people isolated by geography, conflict or disaster.

But this also comes with risks, and it doesn't mean you or your community need to agree with their opinion and approach. You have a right to question, request changes to, or reject their use of digital technology. If the organization doesn't act on your concerns, you have the right to make a complaint. Understanding these rights can help you hold humanitarian organizations to account for applying them.

Rules humanitarians must comply with

To claim your rights in relation to digital technology, you can refer to a number of rules, standards and commitments which humanitarian organizations are bound by.

Humanitarian principles

All recognized humanitarian organizations commit to four fundamental humanitarian principles. You could refer to these to argue for alternatives to digital services and digital data collection methods, for better protection for your data, for support to help you use digital tools safely, or for clarity about who gets to see information you provide.

Principle	What this means for the use of digital technology
Humanity – Protect life and dignity; relieve suffering wherever it exists.	Technology must not cause harm; must not prevent assistance reaching the most vulnerable.
Neutrality – Don't take sides in conflicts or political disputes.	Data must not be shared with authorities or others that may endanger people.
Impartiality – Help people based on need alone, without discrimination.	Technology must not exclude people from assistance, for instance through language or lack of digital skills.
Independence – Keep humanitarian action free from outside influence.	Commercial interests must not influence the design of solutions.

Example

An organization would violate humanitarian principles if a government or armed group accesses data on individuals it wants to target for violence or deportation, or if an abuser was able to see the identity of a person who reported them. A community could argue that digital services that are not accessible to people with disabilities are contrary to humanitarian principles.

Humanitarian standards

A text called the Sphere Handbook sets out core principles and standards that are internationally recognized as a reference for the quality and accountability of humanitarian action. These build on the four humanitarian principles outlined above. You can refer to these 'Sphere standards' to argue for organizations to involve you in decisions on the use of digital technology, ensure the technology doesn't expose people to harm, make it accessible to marginalized groups, and enable you to raise complaints safely.

Standard	What this means for the use of digital technology
People and communities can exercise their rights and participate in actions and decisions that affect them.	Organizations should design digital services with communities and marginalized groups, and maintain non-digital alternatives where needed.
People and communities access timely and effective support in accordance with their specific needs and priorities.	Digital services should address barriers faced by marginalized groups, including barriers of accessibility linked to language, literacy, disability, digital skills and cost.
People and communities access support that does not cause harm to people or the environment.	Organizations should assess and monitor risks to individuals and provide safeguards against digital harm.
People and communities can safely report concerns and complaints and get them addressed.	Organizations should provide channels for people to raise concerns and complaints about digital services and the use of digital technology.

The standards set out in the Sphere Handbook are not law, but they remain a powerful reference, because an organization's reputation depends on meeting recognized standards. In addition, many international organizations publicly certify that their work is in accordance with the Core Humanitarian Standard, which is part of the Sphere Handbook. This makes it all the more powerful if you question whether the way these certified organizations use digital technology is in line with these standards.

Example

An organization that failed to consult community members before setting up digital services would not be fully applying Sphere standards. An individual or community could also criticize it with reference to the standards if women or older adults were unable to use a digital service because it wasn't available in their language or in a non-text format.

For more information about humanitarian principles and standards see:

https://spherestandards.org/handbook/
https://www.corehumanitarianstandard.org/
https://www.unocha.org/publications/report/world/ocha-message-humanitarian-principles-enar

Data protection laws

Humanitarian organizations must comply with data protection laws in the country they are based in, the country where they operate, the country of anyone they gather **data** on, and the country of the agency or government that funds their work.

If your country has laws or regulations on data protection, you can report any violations by an organization operating there to the regulatory authority. You could ask local officials, a lawyer or the humanitarian organization itself for this information.

The legal basis may be a general article in the national constitution establishing a right to **data privacy**, or it may be a specific data protection law. A law should specify the body responsible for receiving complaints, which may be a data protection council or commission linked to the ministry of commerce or ministry of information and communication technology.

Examples

In **Kenya**, the right to data privacy is protected by the constitution, the Data Protection Act and regulations. The Office of the Data Protection Commissioner (ODPC) is the regulatory body and investigates complaints. Penalties include fines, criminal charges and compensation of victims.

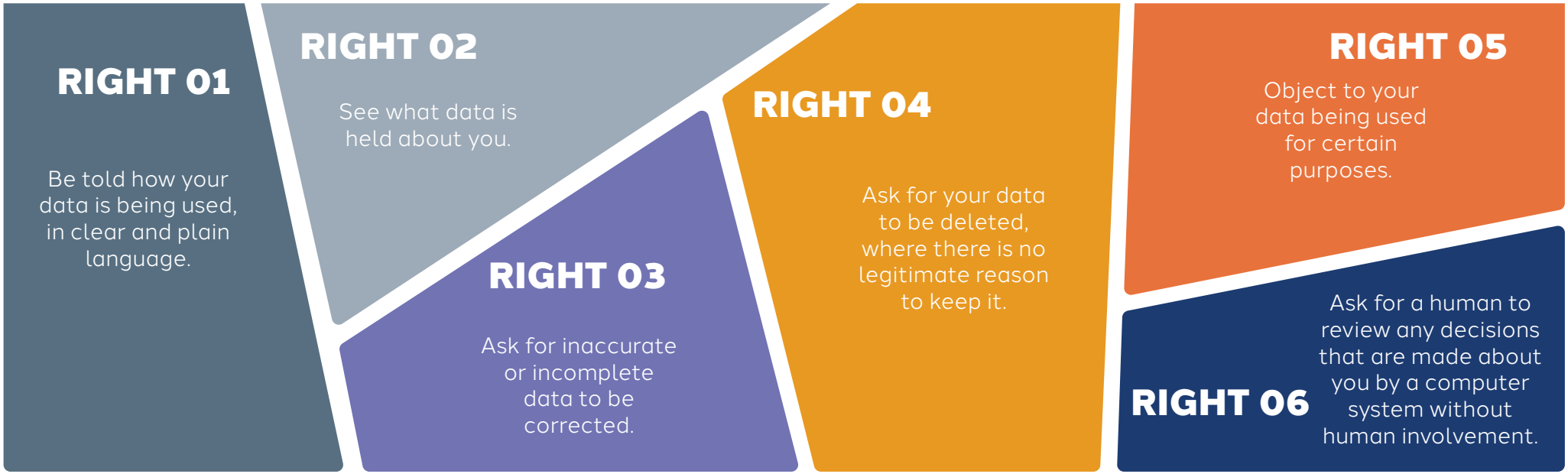
In **Colombia**, personal data protection is a right under the constitution, the General Data Protection Law and decrees. The Superintendence of Industry and Commerce (SIC) is the regulatory body but will only consider complaints if the organization holding the data fails to give a satisfactory response within 15 days.

Lasting conflict and upheaval undermine the functioning of legal frameworks. If the data protection framework in your country is not known to be effective, **you may have to rely on the data protection standards of humanitarian organizations themselves.**

Data protection standards

For simplicity, most humanitarian organizations that work in several countries apply broadly the same data protection standards wherever they work.

Under these standards you have the right to:



Your informed consent is generally needed

An organization must have a legal basis for recording or processing your data. One legal basis is "informed consent". This means that they ask you if you agree to this, they give you all the information you need to decide, and you are free to say no. You have the right to withdraw your consent at any time.

The organization doesn't need your consent if they need to record or process your data in order to protect your rights or the rights of others, to act in the public interest or to comply with the law.

Organizations must consider the risks to you

But the organization must always consider the risks to you when using or processing your data, and take reasonable steps to protect your privacy. It must also ensure that it collects and processes as little data as possible to achieve its humanitarian goals, only holds that data for the shortest possible time, and only uses it for humanitarian purposes. If your data is lost, stolen, or accessed without authorization, the organization should take steps to inform you and relevant authorities where this could put you at risk.

Examples

When large numbers of people are forcibly displaced in a short period, an organization may collect a lot of **personal information** about their situation and needs in order to assess what type of support services to provide them. Under data protection standards, any personal information that is not relevant to delivering those specific services should then be deleted.

The right to make a complaint

If you think an organization has breached these obligations, you have the right to make a complaint, as an individual or collectively. **Humanitarian organizations should provide a means for you to make a complaint or give feedback confidentially and safely.** You can also complain to the organization's headquarters or to its donor or national oversight body, or to a national data protection authority.

You may want to refer to the principles, standards and laws mentioned in this unit when making a complaint.

You can find guidance on how to make a complaint here: UNIT 9. HOW TO REPORT A PROBLEM

Unit 3

How should community members be involved?

- The principle of human-centered design, which should guide community involvement
- The structure and aims of community involvement and what to expect at each stage
- How to make your participation effective for your community
- What you should be able to expect even when conditions are not ideal

The key things to know about community involvement in the design of digital technology

Humanitarian organizations are expected to involve community members in the design of digital solutions to community problems. This is called human-centered design.

Vulnerable and marginalized community members should be actively involved, to understand everyone's needs, wishes and challenges.

Digital and non-digital solutions should be considered, and services for anyone who can't use a digital solution.

Sometimes the choices available are limited by decisions that have already been made. You have a right to know what was decided and why.

At the very least, you should have an opportunity to give your honest opinion on the relevance of the digital solution proposed, how well it works, and the possible benefits and risks.

Unit 3. How should community members be involved?

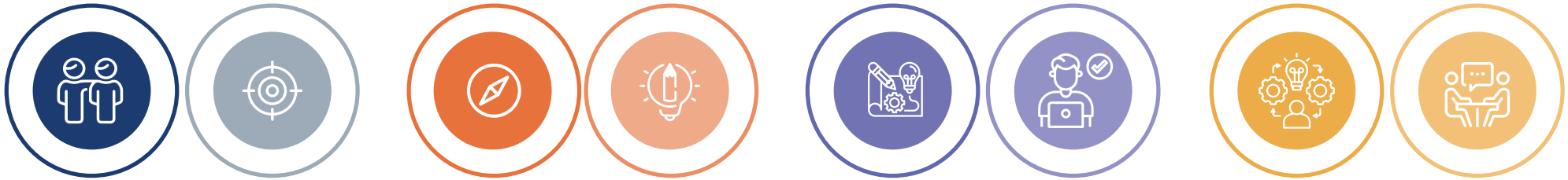
What to expect: human-centered design

Communities should be involved when a humanitarian organization develops and implements a project that uses digital technology to help solve their problems. Their involvement can take different forms, but the basic principle is that decisions at each stage should center on the humans, not the technology. This is often called **human-centered design** (HCD). Essentially this means that the community, including its more vulnerable or marginalized members, should be actively involved at each stage to help determine - and ideally even co-design - the solution.

Sometimes time constraints or safety concerns in an emergency limit the scope of this involvement: a smaller number of people, a shorter consultation period, or remote collaboration not face-to-face. But **the principle remains that the community should always be actively involved.**

This is an ongoing process of community perspectives and reactions feeding continuous learning, adaptation and improvement of the proposed solution.

Human-centered design typically involves 4 stages



Discover and understand | **Explore and ideate** | **Prototype and test** | **Implement and evaluate**

1. Discover and understand

The aim at this stage is to build a solid foundation of understanding to base later decisions on. The organization should consult community members about:

- People's real problems and priorities, from their own perspective.
- Which groups experience exclusion and inequality.
- People's access to and familiarity with digital technology and how they feel about it.
- Preferences between digital and non-digital options.

At the end of this stage, the organization and community members should have a shared understanding of what problems they are seeking a solution for, and where digital technology might be effective. After this stage non-digital solutions should also be considered.

2. Explore and ideate

The aim at this stage is to start thinking about solutions to the problems identified. The organization should involve community members in a creative process (ideation) that translates the findings of stage 1 into:

- A clear problem statement and agreed priority for the community.
- A number of options that seem relevant and feasible, and their benefits and risks.
- High-level features or functions that the solution should have to be useful for the users.
- An agreed strategy for community participation in the following stages.
- Clarity on which ideas should not move forward.

This stage should also identify options for non-digital alternatives for groups that may not be able to engage.

3. Prototype and test

The aim at this stage is to develop early versions of the solution (prototypes) and gather feedback from the intended users. The organization should involve community members multiple times, to:

- Provide feedback on the solution design as it is presented.
- Identify new functions that are missing.
- Give feedback on how easy or difficult initial and successive versions are to understand and use.
- Spot any risks that were missed in the previous stages.

This is also an opportunity to think of and share new ideas.

4. Implement and evaluate

The process of human-centered design should not stop when the solution is launched. The organization should closely monitor how the tools are used, including through feedback from users. It should provide a means for community members to share what they experience, and it should act on that - whether by making adjustments, launching new versions, or communicating why certain changes have not been made.

If you take part in this process, you can ensure the best result for your community by...

- ✓ Presenting an honest picture: for example, don't minimize problems or exaggerate digital skills.
- ✓ Helping to ensure that less powerful individuals can make their views heard.
- ✓ Challenging any incorrect assumptions: you are the experts on your own needs, priorities and experience.
- ✓ Asking for more information or practical examples if you need them to understand possible risks and benefits.
- ✓ Ensuring that if the conclusions don't fit with your understanding, you don't accept them.
- ✓ Asking about non-digital as well as digital solutions.
- ✓ At each stage, asking about the timings of next steps and how community members will be kept informed.

What it means to participate in designing a digital solution

How an organization involves community members will vary, especially in an emergency when there is time pressure to get services to the people who need them. In such cases, in-person co-design activities may not be feasible - but the organization still needs information from you as community members as a basis for developing its solution.

Whether through phone calls, online consultation or even radio shows, at the very least the organization needs community perspectives on the choice and relevance of the digital solution proposed and its benefits and risks. It should **find ways to collect feedback from you as community members so that the final design is based as far as possible on your needs, wishes and challenges.**

At any of the 4 stages, you should expect

- ✓ Participants from diverse sections of the community, and both women and men
- ✓ A safe, private space for discussion
- ✓ Accessible consultation, in the languages and formats participants are comfortable with
- ✓ Opportunities to agree and disagree, and to ask questions
- ✓ Information on the outcomes
- ✓ Explicit consideration of risks for community members

Ideally your participation should also be:

- Timed to suit your availability and preferences
- Compensated in some way
- Face-to-face or with human support where you need it

At stage 1. Discover and Understand, you should expect

Consultation through workshop exercises or surveys to understand people's habits, perceptions, challenges and wishes
Space to share your own perspectives

You should not expect:
• The organization to impose its assumptions on you

At stage 2. Explore and Ideate, you should expect

A practical introduction to digital technology, if you need it to prepare
Additional information about which problem the organization hopes to find a solution for, as a basis for participating in the discussion on your terms
Space to express your ideas freely and safely on how you would want to solve the problems you and your community face

You may find participation is:
• In separate groups of men and women, or more and less digitally confident participants
• Open discussion where even the wildest ideas are considered, as a way of encouraging the creative thinking that can result in unexpectedly innovative solutions
• Hard when time is limited, or if insecurity prevents people traveling to attend

At stage 3. Prototype and Test, you should expect

To be shown physical models of solutions that you can touch or interact with; these may be in digital form (for example on your phone) or just a sketch on paper showing how it would look on a digital device
To be asked for your thoughts and reactions, perhaps multiple times as the solution is improved on the basis of your successive responses
Your honest opinion to be valued, including on any aspects of the solution or how it would be implemented that would need additional training

What participation should not be:
• A test of your knowledge or digital skills; instead you test how well the different versions of the solution work for you

At stage 4. Implement and evaluate, you should expect

Information and training for people who will use or be affected by the solution
A way of giving feedback, reporting problems and getting information about how the organization acts on the reports and feedback received

What participation should not be:
• A one-time involvement: over time, changing needs and circumstances may make aspects of the solution less relevant, and you should have the chance to raise that and get a response

The principles are the same even when the process is more limited

In practice, the process may not be as structured as this: some stages may be combined and the whole process may happen very quickly. **The important thing is that each stage is considered,** so that if one stage is missed or given less attention, it is with good reason.

And in practice, most organizations will not involve every community in all stages of the process. For various reasons, **some aspects of the solution may already have been decided by the time your community is consulted.**

Funding may already be agreed.

Any decisions written in the funding agreement are hard to change. These typically include the duration of the project, the funds available, the general problem the project aims to solve and who it should benefit in the community.

The digital solution may already be decided.

This happens where an organization has decided to reuse a digital solution that has been developed and implemented in another context. The tool or the way it is used should still be adapted to your community.

A digital platform for the solution may already be identified.

Commercial platforms like WhatsApp or Facebook have their own policies on data protection, which may limit the options available to the organization for keeping users' data safe.

Data sharing agreements may already be signed.

Government authorities in your country or another humanitarian organization may be able to see users' data.

The digital solution may be launched without consultation.

Here most of the decisions will already be made. But the organization should still monitor use, provide ways for you to give feedback or report problems, and act on the feedback you give, or explain why not.

The minimum you should expect even in a more limited process

Where decisions have already been made, it will limit the range of options the organization consults you on - but the principle of human-centered design still applies. You have a right to:

- ✓ Know what has already been decided.
- ✓ Know the reasons for those decisions.
- ✓ Say if you feel the impact of any decision will be harmful.
- ✓ Participate in decisions on what should be changed to make the solution safe and relevant for your community.
- ✓ Give feedback or raise any concerns.
- ✓ Know what has been done to address problems raised.

You can find guidance on how to report a problem here: **UNIT 9. HOW TO REPORT A PROBLEM**

Unit 4

Common risks and how to avoid them

- What could go wrong
- How it could happen
- What YOU can do
- How organizations can prevent it

The key things to know about common risks and how to avoid them

There are 3 common risks you may face with digital technology:

Other people see your data and use it to harm or embarrass you.

You receive incorrect or harmful information.

A computer system misinterprets your information.

To reduce these risks, you can be careful what information you share, delete messages and search history, and ask for your data to be deleted. **The organization can** store your data securely, record as little information as possible, and ensure human oversight of automated decisions and communication.

Unit 4. Common risks and how to avoid them

Risk 1. Other people see your data

*If information about you — like your name, phone number, photo, messages or your **search history** — is not securely stored, someone else could see or download it. They could use it to pretend to be you, to gain your trust, or to monitor or harm you.*

Relevant for

1. **Apps** you log into
2. Apps used to communicate with humanitarians
3. Services an organization registers you for
4. Questions to a **chatbot**
5. Any information you share **online**

How it could happen

1. An organization stores your **data** on a computer many people can access
2. Data is not **encrypted** or is transferred on an insecure connection
3. Your text or voice messages to a chatbot, friends or family are stored on a shared phone
4. The commercial app or platform does not commit to keeping your data private
5. The service provider shares data with a government or other organization

What you can do

1. When possible, choose apps that don't require you to register or log on
2. If you must register, share as little **personal information** as possible
3. Be careful who you let use your phone
4. Only register on a shared phone if you fully trust the other user
5. Never tell anyone your password
6. Delete the app and clear your **search history** after each conversation
7. Ask for your data to be deleted

Ask organizations to...

1. Tell you how they will keep your data safe and who can access it
2. Design services so users don't need to register or log in
3. Automatically wipe all data from the phone once a conversation ends
4. Ensure the commercial app or platform used doesn't have access to your data
5. Ensure individual users' data can be traced and deleted on request
6. Provide users with mobile phones for their own use

Risk 2. You receive incorrect or harmful information

Chatbots *and automated services cannot apply human judgment and often make mistakes — especially when communicating in a language not widely used in global trade or when information comes from a different context.*

Relevant for	How it could happen	What you can do	Ask organizations to...
1. Chatbots 2. Any automated information service	1. Responses are based on reference information in a different language or from a different context than your own 2. The organization does not monitor the chatbot or service for errors and potentially harmful responses	1. Be aware that a chatbot or automated service cannot apply human judgment and the information may be wrong or harmful 2. If in doubt, check with someone you trust before acting on any information provided	1. Clearly state if an information service is automated 2. Ensure continuous monitoring to identify and correct risks of errors and potentially harmful responses 3. Provide a human information service as backup

Risk 3. A digital system makes mistakes in processing your information

Artificial intelligence *is faster than human judgment at confirming a person's identity or whether they have certain characteristics. But it makes mistakes, and its decisions can be hard to challenge.*

Relevant for	How it could happen	What you can do	Ask organizations to...
1. **Biometric** registration 2. Automated decision-making, for example on eligibility for assistance	1. Facial recognition is often less accurate at identifying someone with dark skin 2. Electronic fingerprint recognition can become less accurate over time 3. Your **data** could be entered wrongly or confused with someone else's 4. **AI** only knows the data it is trained on, which may not be relevant to you 5. **AI** can simply make a mistake, but humans may assume 'the computer knows best'	1. Ask for an alternative to biometric registration 2. Ask for human verification of any decision that wrongly identifies you	1. Use an alternative to biometric registration 2. Ensure a human can quickly intervene in cases of misidentification 3. Have a human quickly review any AI-based decision that is challenged 4. Ensure continuous monitoring to identify and correct errors in AI decision-making

The risks described above are some of those you are most likely to face. But other risks can also arise. If you want to protect yourself, it's always worth asking:

- ✓ What happens to your data, who can see it, and whether you can ask for it to be deleted
- ✓ What the organization will do to protect you against risks
- ✓ For a non-digital alternative if you are not satisfied you will be safe

You can find more information on questions to ask here: UNIT 7. WHAT YOU HAVE A RIGHT TO KNOW

Unit 5

What digital risks look like in practice

- Risks related to different types of digital technology
- How the way the organization uses the technology affects your risk
- Possible consequences when things go wrong

The key things to know about what digital risks look like in practice

Some of the digital technology used in humanitarian action carries specific risks.

AI used for chatbots or to identify people using biometric data can make mistakes.

Chatbots, mobile money systems and information apps store data on you that could be used against you.

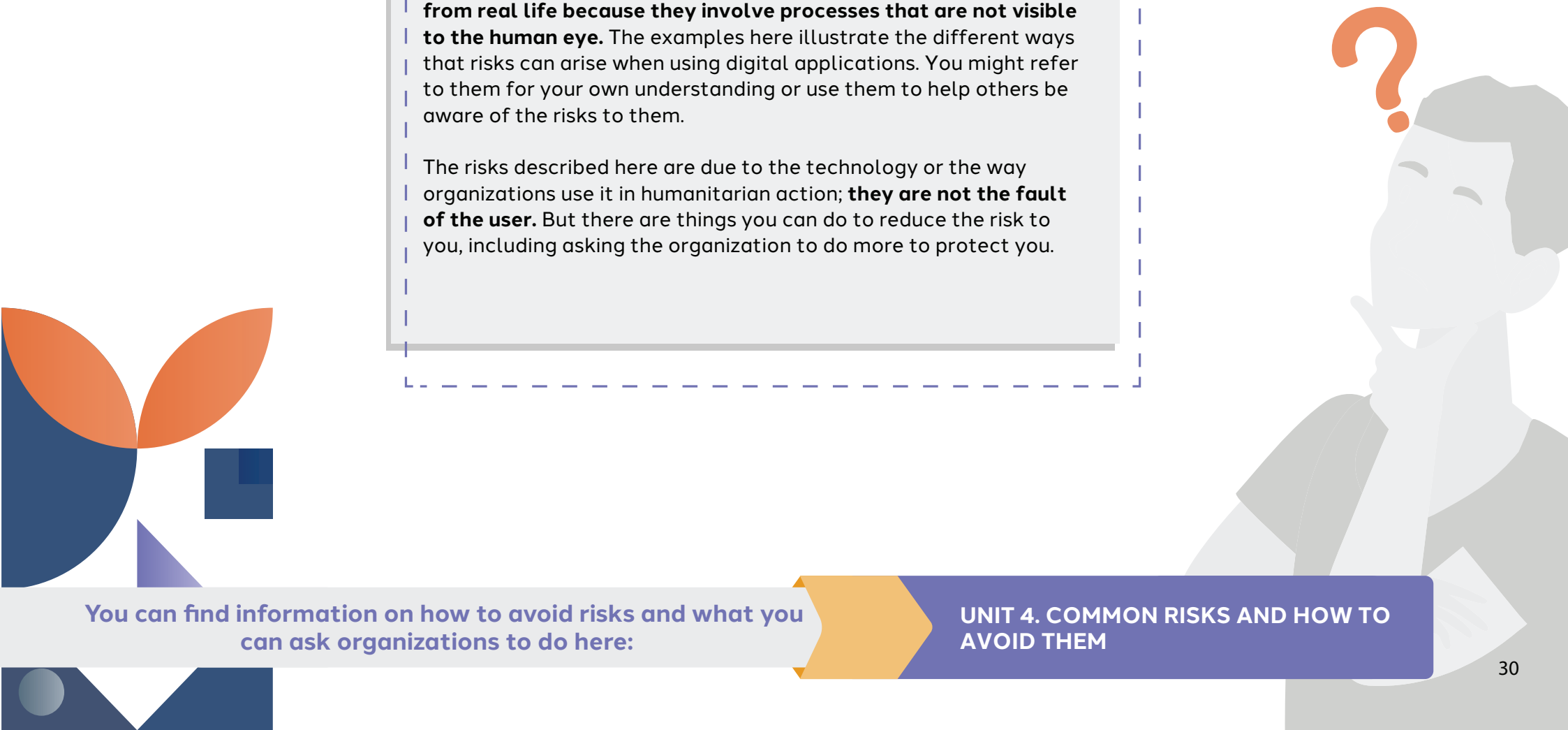
This can have serious consequences for you. Organizations have a responsibility to recognize and manage these risks in order to protect you.

Unit 5. What digital risks look like in practice

How to use this information

Digital technology and the risks it entails can seem disconnected from real life because they involve processes that are not visible to the human eye. The examples here illustrate the different ways that risks can arise when using digital applications. You might refer to them for your own understanding or use them to help others be aware of the risks to them.

The risks described here are due to the technology or the way organizations use it in humanitarian action; **they are not the fault of the user.** But there are things you can do to reduce the risk to you, including asking the organization to do more to protect you.



You can find information on how to avoid risks and what you can ask organizations to do here:

UNIT 4. COMMON RISKS AND HOW TO AVOID THEM

Example 1: **An AI chatbot for sensitive information and feedback**

An organization supporting women and girls launches a new AI chatbot to provide information about women's health and rights. Women and girls can access the chatbot on a smartphone to ask questions and to ask for help if they are in danger. The chatbot responds immediately and like a human, as if the user was chatting with a friend. The chatbot can understand them when they type or speak their own language, so they don't have to translate their questions into another language. It uses **artificial intelligence** to find information related to the question and provide an answer, which it translates into the user's language. If a user says they are in danger or asks for help, the chatbot sends an alert to the organization providing the service; a human may then contact the user to offer assistance.

What can go wrong

- **The conversation with the chatbot may remain visible on the phone after the app is closed.** Someone else who uses the phone may be able to read or listen back to the conversation and know what questions were asked or that the user asked for help. In some situations that might be embarrassing; in others it could be dangerous for the user.

- For example, **it could be dangerous if an abuser sees that their victim has shared information about the abuse.** If the user's questions to the chatbot relate to abortion or same-sex relationships, in some contexts that could put them at risk of violence or arrest.

- **If the user has to identify themselves, for instance by sharing their name and phone number to access the app, then their identity will be stored** by the organization providing the chatbot. If that data is not securely stored, someone who should not have access to that information might be able to identify the person asking questions about sensitive subjects or saying they have been abused.

- **Because the answers are provided by a chatbot not a human, users could receive responses which contain errors** or are not appropriate for the user's context. Acting on these responses might be harmful for the user or for other people.

- **Because the translation is done by a computer not a human, the chatbot could misunderstand the question or mistranslate the answer.** Again, this could result in the user receiving confusing, inaccurate or harmful information.

Example 2: **Aid registration using people's biometric data**

A humanitarian agency registers community members to receive humanitarian aid by taking an electronic record of their fingerprints, eyes or faces (known as '**biometric data**'). This means that people don't need to show ID documents to prove they are eligible for assistance, which is helpful for instance for people who have lost their documents in an emergency. It also means that nobody else can pretend to be them in order to receive aid they are not entitled to.

What can go wrong

- **People's biometric data is stored together with their identity in an electronic database.** It could be stolen by **hackers**, or accessed by staff of the organization or its data storage providers, or shared with civilian or military authorities nationally and internationally.

- **As well as identifying aid recipients, that data can be used to target individuals for violence and intimidation or to track their movements.** Facial recognition software uses biometric data to identify an individual from a video or photo, and is widely used by police and border security agencies.

- **The technology can make mistakes: people can be wrongly denied assistance because the computer fails to recognize their fingerprint or face.** Facial recognition software is known to be unreliable in identifying people with dark skin.

Example 3: **Mobile money**

Mobile money **uses electronic transfers to give people access to money without needing a bank or a bank account.** This means that women and others who may not usually control the family finances, can receive money directly and decide how to spend it. A humanitarian organization registers women in a remote community for mobile money, and transfers money each month, notifying them by **SMS** or through an app.

What can go wrong
✸ **If the woman registered for mobile money can't read, or can't read in the language used in the messages or the app, she won't know how to access the money.** If she can't read the words, she may not know which number is her balance and which number is the money she has received. If she can't read numbers, she won't know how much money she has. She may have to rely on someone else to tell her, and that person might steal her money.
✸ **In a remote area, mobile money agents may not often be available to help, and may not speak the woman's language to offer real assistance.** If she doesn't get the support or training to use the system, she may need to ask for help to withdraw cash or use mobile money to buy something. She may give her password to the shopkeeper or another shopper to make the transaction, and they might steal her money.
✸ **If she registers for mobile money with the number of a phone she shares with someone else, that person could steal her money.**

Example 4: **Mobile apps for migrants**

Mobile apps provide migrants with verified real-time updates on safe routes, shelters, legal aid and other key topics. This makes them less reliant on people smugglers and enables them to avoid unsafe crossings, detention, fraud and other harm.

	What can go wrong
✸	**Using the app could expose migrants to targeting by traffickers and criminal groups if phone data is compromised.** Traffickers could use stolen phones to extort money from families back home and threaten harm if their demands are not met.
✸	**Border authorities could monitor app activity in order to detain migrants or refuse them entry.** If a migrant is stopped or detained, having the app on their phone could also raise suspicion or place them at risk.
✸	**Migrants often use shared or second-hand phones; data breaches could expose their travel history and past or future routes.** Phone theft may also leave them vulnerable to identity theft or fraud.

Unit 6

How to spot unsafe uses of digital technology

Unit 6. How to spot unsafe uses of digital technology

Below is a list of 'red flags' you can use to quickly spot when humanitarian use of digital technology is unsafe.

- No risk assessment of specific harms linked to use of digital technology
- Not available in the languages community members speak and understand
- No accessible, confidential complaint mechanism about digital tools
- Digital-only services with no alternatives
- Users don't have a real opportunity to refuse consent or be properly informed before they give it
- Risks to vulnerable individuals not assessed
- Marginalized groups not informed or involved when technology is designed
- Sensitive data collected without enhanced protection
- **Biometric data** collected without understanding context risks
- Inaccessible to people with disabilities or less literate individuals
- **Personal data** shared across agencies without users' consent
- Commercial platforms with no **data protection** assessment
- Accessible training not provided for users with low digital skills

Unit 7

What you have a right to know

Questions you could ask a humanitarian organization about how they intend to use digital technology in your community, in order to understand the risks and opportunities and what you can do about them

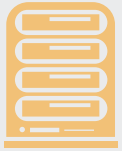
The key things to know about questions to ask

You have a right to information about the proposed use of digital technology, including:

How the community will be consulted

Details of the project

Details of the technology used



Risks and data protection

Channels for reporting any problems

Unit 7. What you have a right to know

How to use these questions

The person you are in contact with may not have all the information you need; they may not even work for the organization implementing the technology. If they work for a different organization, for instance a local organization or a user research company, they may not be responsible for providing the information you need. In that case you have a right to ask the organization implementing the technology to contact you to provide the answers.

Of course, you don't have to ask all the questions here; choose those that seem relevant and adapt them as you think appropriate. You will also have other questions of your own. **You may want to discuss collectively what questions you want to ask as a community before you talk to the organization, and note them down for reference.**

It can be useful to keep a record of the answers to refer to later.

You can find a form to record key information here:

UNIT 8. INFORMATION FORM FOR HOLDING AN ORGANIZATION ACCOUNTABLE

This is information that you have a right to know. You have a right to receive the information in a way that is accessible to you and to other community members. That means that it should be provided in a language community members understand, in spoken form and face to face if preferred and using pictures or graphics if needed to make the meaning clear. You should have the opportunity to ask questions and receive answers about the information provided.

Questions about the consultation process

- ✓ Was anyone from this community involved in designing this product or service?
- ✓ Was anyone from this community involved in testing how well this product or service works for community members?
- ✓ What decisions will you make with information from consulting community members?
- ✓ When will you share the findings of the consultation with us?

Questions about the project

- ✓ What is the project end date? Is it fully funded up to that point?
- ✓ What will happen to the technology at the end of the project? Will another organization take over responsibility for it?
- ✓ What will happen to our data at the end of the project?

Questions about the technology and how to use it

- ✓ If you have used this technology in other places, did it have any harmful impact? How do you plan to avoid that here?
- ✓ Why do you feel this technology can be helpful to this community? What evidence or previous experience suggests this?
- ✓ Where can I find more information about this technology?
- ✓ What information or training is available to help me use the technology?
- ✓ Is that information or training available in my language and in a format I can understand?

Questions about how the organization will protect your data

- ✓ Who will be able to see any information I share? For example, will you share my **data** with government authorities? Will your technology partners be able to see my data under their own data privacy rules?
- ✓ What will the organization do with any information I share?
- ✓ How long will the organization keep any information I share?
- ✓ How will the organization keep my information confidential?
- ✓ Will the organization delete my information later if I ask them to? How would I make that request?
- ✓ Can I get the same assistance without using a digital tool?
- ✓ Can I get the same assistance without giving you my personal details?

Questions about information you need if there's a problem

- ✓ Who in your organization can I go to if I have a problem? How do I contact them?
- ✓ Where (in which country) is your organization's head office? What are the contact details?
- ✓ Which body in that country is responsible for ensuring that organizations like yours apply laws and standards?
- ✓ Who is the donor for this project?
- ✓ Does your organization have Core Humanitarian Standard certification?
- ✓ Is your organization a member of a cluster or other humanitarian coordination group?
- ✓ Which body in my country is responsible for ensuring that data protection standards are met? What are the contact details?

Unit 8

Information form for holding an organization accountable

Unit 8. Information form for holding an organization accountable

You can use this form to keep a record of information to refer to later. This could be helpful:

- ✓ As a reminder, if there are long gaps between contacts from the organization
- ✓ As a record for other community members
- ✓ As a record, if the organization doesn't do what it said it would
- ✓ As a reference, if you need to make a complaint

INFORMATION ABOUT THE PROJECT

Is this a pilot project?

Project end date

Is the project fully funded up to that date?

Handover planned after project end date?

Details of organization expected to take responsibility after project end date

Data protection after project end date?

Continued service after project end date?

You can find a list of questions you could ask a humanitarian organization about how they intend to use digital technology in your community here:

UNIT 7. WHAT YOU HAVE A RIGHT TO KNOW

REGULATORY AND ACCOUNTABILITY FRAMEWORKS

Does the organization have Core Humanitarian Standard certification? ☐ Yes ☐ No

If it does, then if the organization doesn't give you an accessible means to report a problem safely and confidentially, you can complain to the CHS Alliance at the address complaints@chsalliance.org.

Cluster/coordination group membership

National body in your country for regulating data protection standards

Contact details

Contact details

CONTACT DETAILS FOR REPORTING A PROBLEM

Organization's country office

Name

Email

Phone number

Physical address

Best way to report a problem

CONTACT DETAILS FOR REPORTING A PROBLEM

Organization's head office

Name

Email

Phone number

Physical address

Best way to report a problem

CONTACT DETAILS FOR REPORTING A PROBLEM

Donor agency

Name

Email

Phone number

Physical address

Best way to report a problem

CONTACT DETAILS FOR REPORTING A PROBLEM

Regulatory body in the organization's own country

Name

Email

Phone number

Physical address

Best way to report a problem

Unit 9

How to report a problem

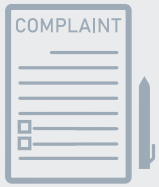
- Your right to report or make a complaint about harm caused by humanitarian use of digital technology
- What information you need
- What steps to take
- How to write an email or letter reporting a problem

The key things to know about reporting a problem

You have a right to report a problem; it may be most effective to do this collectively.

The organization must give you an accessible way of reporting a problem, must keep your identity confidential, and should give you a response.

If that doesn't solve the problem, you can make a complaint to a higher body, for example the donor or your national authorities.



Your report or complaint should contain what happened, the impact, who is affected, and any evidence you can provide.

To support your case, refer to the rules for how humanitarians use digital technology.

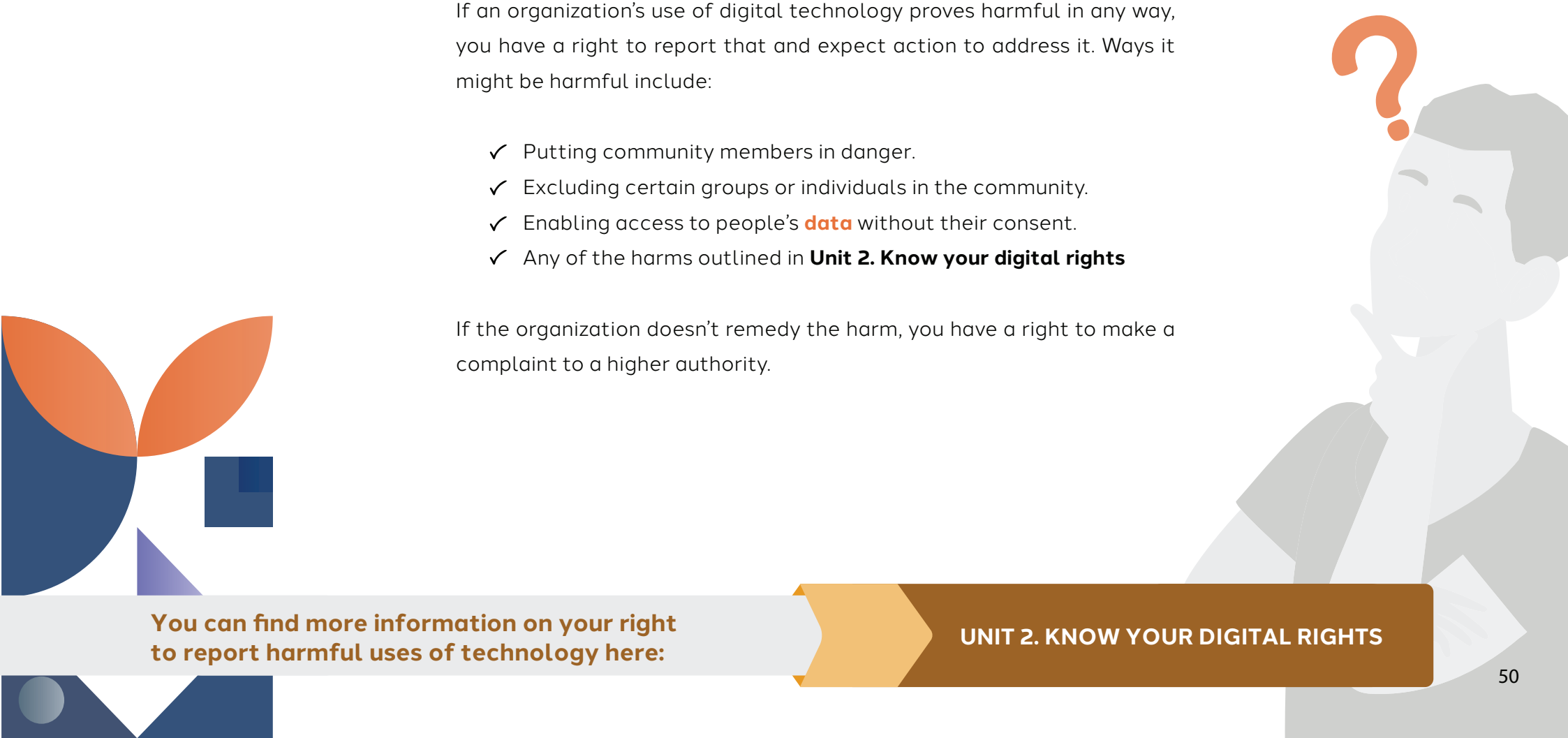
Unit 9. How to report a problem

You have a right to report a problem or make a complaint

If an organization's use of digital technology proves harmful in any way, you have a right to report that and expect action to address it. Ways it might be harmful include:

- ✓ Putting community members in danger.
- ✓ Excluding certain groups or individuals in the community.
- ✓ Enabling access to people's **data** without their consent.
- ✓ Any of the harms outlined in **Unit 2. Know your digital rights**

If the organization doesn't remedy the harm, you have a right to make a complaint to a higher authority.



You can find more information on your right to report harmful uses of technology here:

UNIT 2. KNOW YOUR DIGITAL RIGHTS

What the organization cannot do

The organization CANNOT:

- ✓ Ask you to stop reporting problems or making complaints.
- ✓ Prevent you from contacting higher authorities about the problem.
- ✓ Exclude you from receiving assistance because you made a complaint.

There are 3 steps to reporting a problem

1. Prepare the information you need
2. Report the problem to the organization
3. If that doesn't work, make a complaint to a higher authority

Below you can find an example of a letter or email reporting a problem, which you can use as a basis for your own report if helpful.

Step 1: **Prepare the information to report**

Consider reporting collectively

It may be best to prepare this information collectively, ideally including individuals from diverse groups across the community. This can help by:

- ✓ Ensuring you have all the facts before you report.
- ✓ Increasing pressure on the organization to act.
- ✓ Reducing the visibility of individuals affected by the problem.

What information do you need?

- ✓ What is the problem: a short, clear summary of what has happened and why it is a problem
- ✓ Who is affected: which groups of people, potentially with numbers
- ✓ Evidence: this could be a short account of an incident, with dates, and if relevant and feasible, photos or screenshots
- ✓ Reference to organizational commitments: how do the problems compare with how the organization said things would work, or with the rules they must comply with?

It can be helpful to write this information down somewhere so community members can refer to it when needed. You may not need to provide it all when you first report the problem.

If you are reporting about harm done to other people, remember not to use their names or any personal details that could identify them in your report, to protect their privacy. You can report confidentially if you are worried about your safety, but you should let the organization know how to respond. This might be through a named community leader whose contact details you share, or through a community meeting.

You can find information on rules organizations must comply with here:

Step 2: **Report the problem to the organization**

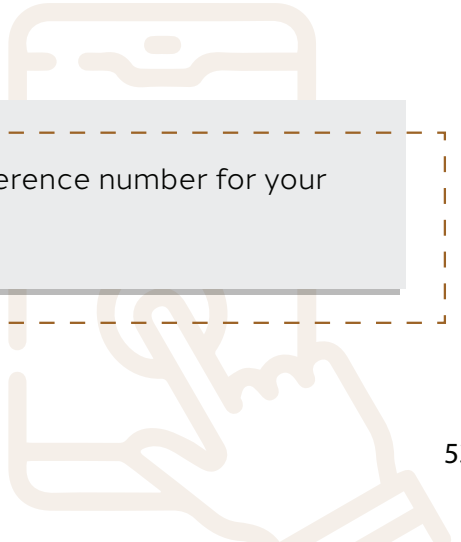
The organization should have a system in place for community members to report a problem or give feedback. This can take different forms: sometimes you submit feedback in writing by email or through a 'suggestion box'; other times you submit spoken feedback, through a phone call or a voice recording or directly to a designated person.

The organization should ensure that the system is accessible to community members. This may mean providing spoken feedback options and enabling people to report and get a response in their own language.

If you report a problem or make a complaint, the organization should always:

- ✓ Give priority to the safety of the individuals involved
- ✓ Keep your identity confidential
- ✓ Inform you about what they have done about it

If you share your contact details, the organization should give you a reference number for your report. You can use this to follow up for information.



Keep a copy of your letter or email before you send it. Ask the organization to give you a reference number so you can follow up.

If the organization doesn't respond, you can report to their head office, the donor, or your national data protection authority.

You can also report confidentially. You do not have to give your name if you are worried about your safety.

There are normally 3 ways to report the problem directly to the organization:

1. Through the feedback system in place for the digital product or service

If one exists, this is probably the first option to try.

2. Through a general feedback system for the organization in your country

The organization may call this a complaints and feedback mechanism or a complaint and reporting mechanism. Whatever it's called, contact details should be widely communicated to community members.

3. Through a general feedback system for humanitarian organizations in your country

In some countries a system exists to enable you to report problems confidentially to an independent body, which then passes your report on to the organization concerned.

Step 3: **Make a complaint to a higher authority**

If the organization doesn't fix the problem, you can make a complaint to another authority that can hold the organization to account.

This authority may have direct power over the organization:
the organization's head office, the donor, the body that oversees humanitarian organizations in its home country, or the body responsible for data protection laws in your country.

Or it may have indirect influence:
a coordination group or 'cluster' in your country that the organization is a member of, or the CHS Alliance.

You have a right to ask the organization for contact details for any of these bodies. You can also find the information through the ministry responsible for coordinating humanitarian action in your country, or **online.**

If it's helpful, you can find a form for recording these contact details here:

UNIT 8. INFORMATION FORM FOR HOLDING AN ORGANIZATION ACCOUNTABLE

Template letter for reporting a problem with digital technology

You can use this template to report problems by letter or email. Make a copy so that you and other community members can refer to it later.

Name / group name (optional):

.....

Our contact details (phone / email / address):

.....

Date:

.....

To (name of organization):

.....

Name of program or digital service:

.....

Dear Sir / Madam,

We are writing to report a problem with [name of digital technology / service] _____, used by your organization in [location] _____

.

We have attached a list of the specific problems. These have affected at least [number] _____ people in our community.

We are asking you to _____.

Please respond to us by [date]_____. If we do not hear from you, we will contact:_____

We ask you to keep our identities confidential.

Yours sincerely,

Checklist of problems

[Tick all that apply, and add details where you can.]

1. OUR DATA OR PRIVACY

- ☐ Personal information about us was seen by someone who should not have had access to it.
- ☐ Our data (name, photo, phone number, fingerprints etc.) was shared without our agreement.
- ☐ Messages or conversations on the app or chatbot can be seen by other people.
- ☐ We were not told what data was being collected or how it would be used.

Details:

2. WRONG OR HARMFUL INFORMATION

- ☐ A chatbot or automated service gave us wrong or harmful information.
- ☐ The information was not in our language, or did not fit our situation.
- ☐ There was no human we could go to instead.

Details:

3. MISTAKES BY A DIGITAL SYSTEM

- ☐ A fingerprint, face or eye scan failed to recognize registered community members.
- ☐ A computer wrongly decided community members were not eligible for assistance.
- ☐ We could not challenge or appeal the decision.

Details:

4. SOME PEOPLE CANNOT USE THE SERVICE

- ☐ The service is not in our language.
- ☐ People who cannot read cannot use it.
- ☐ People with disabilities cannot use it.
- ☐ People without a phone or internet access cannot use it.
- ☐ There is no non-digital alternative.

Details:

5. WE WERE NOT CONSULTED

- ☐ The organization introduced this technology without asking our community.
- ☐ Women / older people / people with disabilities were not asked for their views.
- ☐ We were not told how the technology works or what information it collects.

Details:

Unit 10

What does that mean? A digital rights glossary

Unit 10. What does that mean? A digital rights glossary

A lot of the terms used to talk about digital technology may be unfamiliar, making it hard to understand the risks and opportunities and to ask for improvements. This glossary provides a brief explanation in plain language for some of the key terms you will need to know. Words highlighted **like this** in other parts of the guide are terms you can find in this glossary.

Term	Definition
Account	A personal login you create with a **website** or **app**, usually using an email address and **password**. Your account lets you access services and stores your personal information and activity.
App (application)	A program you can use on a phone, tablet, or computer to do a specific task — like check the weather, send messages, or use **mobile money.**
Artificial intelligence (AI)	Technology that automates tasks normally done by humans, like answering questions, recognizing faces, or making decisions — by processing large amounts of information faster than humans can.
Biometric data	Physical features unique to you that computers can use to identify you — such as your fingerprint, face, or voice.
Chatbot	A computer program designed to have a conversation with you, usually by text. It can answer questions or give guidance, but it isn't a real person.
Data	Any information stored or processed by a computer, smartphone or other **device** — this includes your name, photos, messages, location, and search history.
Data breach	A situation where someone gains unauthorized access to **data**, especially personal or sensitive information.
Data privacy	The safety of your personal information; what **data protection** rules and practices aim to achieve.
Data protection	Rules and practices that keep your **personal information** safe, control who can access it, and give you rights over how it is used.
Device	Any piece of equipment you use to go online or run **apps** — such as a smartphone, tablet, laptop, or desktop computer.
Download	Copying a file, **app**, or **data** from the internet onto a device to use or view it.

Term	Definition
Encrypted	Coded: a way of scrambling information so that only the person it is intended for can read it — like putting a message in a secret code that only the recipient can unlock.
Hacker	Someone who gains unauthorized access to someone else's computer, account, or device, usually to steal information or cause harm.
Informed consent	Agreement, for instance to let an organization have your data, that you give freely and after the organization has given you all the information you need to decide, in a language and format you understand.
Human-centered design (HCD)	A participatory approach to problem solving through learning, improving and adapting solutions in collaboration with the intended users. This approach can be applied to digital and non-digital solutions.
Mobile money	A service that enables you to send, receive and spend money from a mobile phone, without needing a bank account.
Online	Connected to the internet. Being 'online' means your device is actively using an internet connection.
Password	A secret combination of letters, numbers, and symbols used to prove your identity and protect your accounts from being accessed by others.
Personal data (also called 'personal information' or 'personally identifiable information', or PII)	Any information that could be used to identify you as a specific individual, like your name, address, date of birth, national insurance number, employment record or membership of an organization.
Profile	A personal page on an app or website (commonly used on social media) that contains information about you — like your name, photo, and interests. Other people may be able to see your profile, depending on your privacy settings.
Search history	A record of everything you have searched for and websites you have visited, stored on your smartphone or other device.
SMS (also called 'text message')	A short electronic message sent and received on a mobile phone. Basic phones, which cannot run messaging apps like WhatsApp or Telegram to send and receive messages, can use SMS, which is an older technology.
Social media	Websites and apps that let you create a personal profile and connect with others online — sharing photos, opinions, news, or messages. Examples include Facebook, Instagram, and WhatsApp. Anyone with internet access can usually sign up, and what you post can often be seen by a large number of people.
Website	A collection of pages of information hosted on the internet, which you can visit using a browser (such as Google Chrome or Safari). Websites can belong to businesses, organizations, or individuals — for example, a bank's website or a news site.

Unit 11

Where's my data? — A game for understanding about data privacy

Unit 11. Where's my data? — A game for understanding about data privacy

Purpose

To help participants understand, in a personal and memorable way, how easily we can lose control of our information online — and why that matters.

What you need

- ✓ A piece of paper and pen for each participant
- ✓ A bowl, box, or clear space in the middle of the room

Instructions

Step 1 — Introduce the activity (2 minutes)

Tell participants they are going to play a short game about secrets and trust. Keep it light — reassure them that nobody will be forced to share anything they're uncomfortable with. Say something like:

"Think of something mildly embarrassing or personal — something you wouldn't necessarily want a stranger to know, but nothing too private or upsetting. For example: a food you secretly hate, something you've never admitted to enjoying, or a small habit you'd rather keep to yourself."

Step 2 — Write it down (2 minutes)

Ask everyone to write their secret on a piece of paper — without their name. They should not show anyone. Give them a moment to think.

Step 3 — Let it go (1 minute)

Ask everyone to screw their paper into a ball and either throw it into the middle of the room or place it in a bowl or box. Make it fun — throwing works well if the space allows.

Step 4 — Pick one up (1 minute)

Ask everyone to pick up a paper ball — ideally not their own. They should read it silently to themselves.

Discussion (10–15 minutes)

Use the following questions to guide a conversation. You don't need to use all of them — use your judgment.

- ✓ **How does it feel** knowing someone else is now reading your secret?
- ✓ **Do you know where your own secret is?** Who's holding it? How many people might read it before the session ends?
- ✓ **Did you trust the process** when you wrote it down? What made you willing — or reluctant — to hand it over?
- ✓ Now imagine that piece of paper is something you shared **online** — a photo, your location, your date of birth, or a message. **Who might have access to it that you didn't intend?**
- ✓ Once something is out there, **can you get it back?**

Key messages to draw out

- ✓ Once you share information — online or otherwise — **you lose control of it**. You don't always know who has it, where it goes, or how it might be used.
- ✓ Online, this happens **faster and at a much larger scale** than a paper ball in a room. Information can be copied, shared, or stored without your knowledge.
- ✓ It's worth thinking **before** you share: would you be comfortable if a stranger, an employer, or someone you don't trust saw this?
- ✓ **Privacy settings help, but they are not a guarantee.** Platforms, companies, and other people can all handle your **data** in ways you didn't expect or agree to.

Closing (2 minutes)

Collect the paper balls and — importantly — destroy them in front of the group (tear them up). This is a good moment to note that online, **there is no equivalent action**: once data is shared digitally, it is rarely possible to fully delete or retrieve it.

Facilitator notes

- ✓ Keep the tone light and non-alarmist, especially at the start. The goal is to raise people's awareness, not make them anxious.
- ✓ Be sensitive to the fact that some participants may feel uncomfortable — nobody should feel pressured to write anything genuinely personal.
- ✓ The game works best when participants feel safe, so consider running it in groups of the same sex and possibly a similar age and background. Remind them at the start that secrets should be light-hearted and not something they care about deeply.
- ✓ Adapt the discussion questions to the age and background of your group.

About CLEAR Global

CLEAR Global's mission is to help people get vital information and be heard, whatever language they speak. We help our partner organisations to listen to and communicate effectively with the communities they serve. We provide interpretation services, translate messages and documents into local languages, support audio translations and pictorial information, train staff and volunteers, and advise on two-way communication. We also work with partners to field test and revise materials to improve comprehension and impact, and to develop language technology solutions that work for communities. This work is informed by research, language mapping and assessments of target populations' communication needs. We also provide training to support effective humanitarian communication (topics include humanitarian interpreting, communication in emergencies, and plain language). For more information, visit our website or contact us at info@clearglobal.org.

Acknowledgements

CLEAR Global sincerely thanks all the individuals and organisations who supported and contributed to this guide, particularly the civil society experts who generously gave their time. The guide was developed from a concept of Christine Fricke and Milena Haykowska's. Dr Camille Maubert led the scoping study for the toolkit with support from Ellie Kemp, Milena Haykowska, Maria Spychała-Kij and Julián Picotto. Ellie Kemp authored the guide and Victoire Rwicha designed it, with support from Milena Haykowska and Clara Sanchiz. The game in unit 11 is based on one developed by Gender Rights in Technology (GRIT) and described to the author.

This work was commissioned and supported by the UK Humanitarian Innovation Hub and Elrha and funded by UK International Development. This guide represents the views of the authors, which are not necessarily those held by UKHIH, Elrha or the Foreign, Commonwealth and Development Office (FCDO).

CLEAR Global

United Kingdom Humanitarian Innovation Hub

elrha

UK International Development

Partnership | Progress | Prosperity