
Training Handbook

Survivor-centered responses to TFGBV in Kenya

31 JULY - 2 AUGUST **2024**

TRANSFORM DIGITAL SPACES





The enclosed training handbook was developed as part of a training delivered by Moonshot to Kenyan organizations in September 2024 as part of the [Transform](#) program. The content of the handbook reflects the specific needs and requests for support from these organizations.

The material was created to accompany the training sessions, rather than as standalone resources. Concepts were fleshed out and discussed in more detail during the training and through follow-up engagement with the training participants. Despite this, we hope the handbook will still be a useful reference for other organizations working on related topics.

Please note that links within the handbook were last reviewed in September 2024 and there are no plans to review and update them in an ongoing way.



Overview

Between 31 July and 2 August, Moonshot will deliver capacity building workshops to organizations working on TFGBV, online violence, digital democracy, women's rights, and related issues in Kenya. This activity forms part of Moonshot's work on the Transform Digital Spaces (Transform) Activity to help local support organizations develop confidential, survivor-centered, safe, and secure online mechanisms through which all TFGBV survivors may seek services.

The program aims to increase the capacity of these practitioners to provide support to survivors of TFGBV. The training will cover the following core areas:

- 1** Overview of TFGBV with a focus on the Kenyan context
- 2** Online research to build the evidence base around TFGBV in Kenya
- 3** Staff safety and welfare when working on TFGBV, and with potential victims/survivors
- 4** User-centered design for vulnerable audiences
- 5** Digital campaigns to support survivors and bystanders of TFGBV

This handbook provides key insights covered in the training, along with valuable resources and links for conducting safe online research and developing your digital campaigns.

↘ Introduction to TFGBV

▼ Points to remember

📖 Definition

Technology-Facilitated Gender-Based Violence: A threat or act of violence committed, assisted, aggravated, and amplified in part or fully by using information and communication technologies or digital media that is disproportionately targeted at women, girls, and gender non-conforming individuals. It is a continuum of multiple, recurring, and interrelated forms of gender-based violence that takes place both online and offline. (United States Strategy to Prevent and Respond to Gender-Based Violence Globally 2022)

📖 Types of TFGBV

- **Cyber Harassment or Online Harassment:** The use of social media (Instagram, TikTok, meta) and other messaging platforms to degrade, insult, or threaten someone based on their gender or sexuality.
- **Cyberstalking:** Continuous pestering of a person's online presence, communications and physical location using technology.
- **Doxing:** The publishing of someone's personal information to threaten or harass them.
- **Hate Speech:** Any type of speech that is intended to dehumanize or incite violence against a particular group of people based on their race, gender, sexual orientation, or other characteristics.
- **Impersonation:** Assuming someone's identity online to deceive or harass others.
- **Non- consensual distribution of intimate images:** The sharing of explicit images or videos without the permission of the person.
- **Online Gendered Disinformation and Misinformation:** False or misleading gender and sex-based narratives, often with some degree of coordination, to deter women from participating in the public sphere. Both foreign state and non-state actors strategically use gendered disinformation to silence women, discourage online political discourse, and shape perceptions toward gender and the role of women in democracies.
- **Sextortion:** The use of intimate images or videos to coerce someone into performing sexual acts or providing money or other forms of compensation.

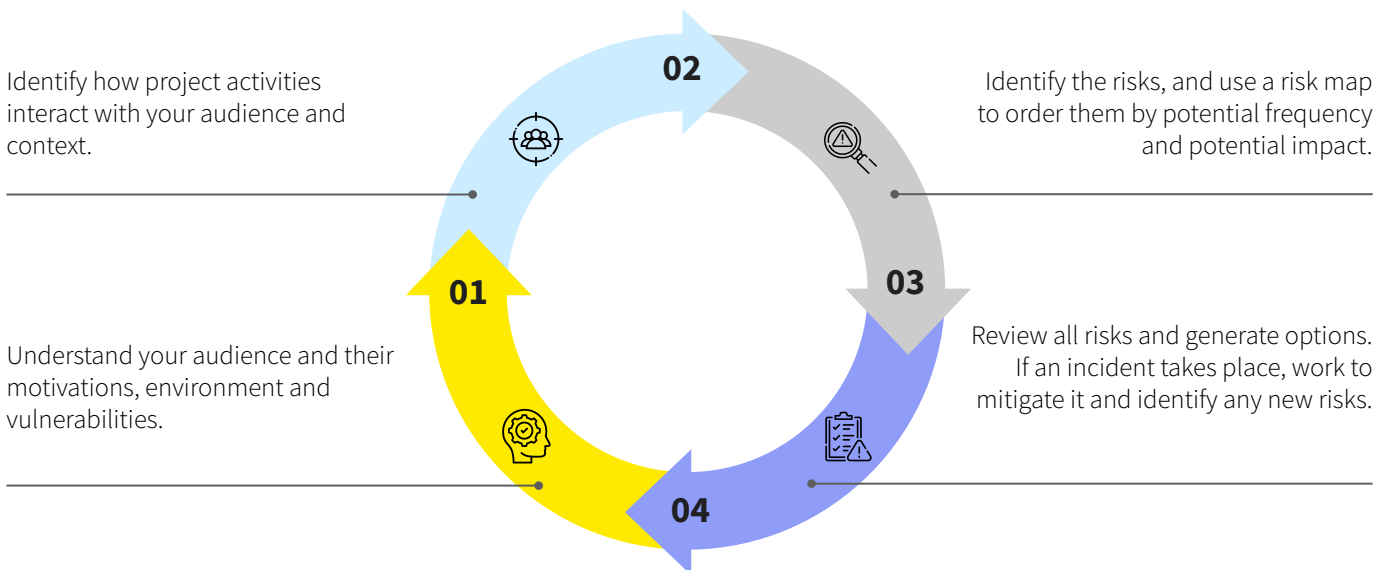
Additional resources [Technology-Facilitated Gender-Based Violence: An Overview](#) Suzie Dunn
[Transform Digital Resource Catalogue](#)

Do No Harm

▼ Points to remember


- Do No Harm is a tool to avoid causing inadvertent harm through the actions of an organisation or the behaviour of its staff.
- Any action - however small - has a risk of doing harm. To 'Do No Harm', practitioners:
 - Understand their audiences, including their motivations, vulnerabilities, and environment
 - Identify how activities can affect audiences in their unique contexts
 - Identify risks, and use a risk map to prioritise them
 - Constantly review risks and generate options
 - If an incident takes place, work together to mitigate it and identify new risks

▼ The principle of Do No Harm



Survivor-centered approach

▼ Points to remember

-  “A survivor-centered approach focuses on the empowerment of survivors by creating a supportive environment for healing. of GBV can regain or strengthen their sense of empowerment when accessing survivor-centered GBV services that uphold these **four guiding principles**:
- 1** Ensure the safety of survivors, including preventing and mitigating further violence;
 - 2** Protect the confidentiality of survivors, including their right for information about them to be shared only with their informed consent and their right to choose whether and to whom to tell their experiences;
 - 3** Demonstrate respect for survivors’ needs and wishes and their right to make their own choices, including those that service providers may find hard to understand or disagree with; and
 - 4** Practice nondiscrimination, ensuring that survivors, in all their diversity, are able to access and receive appropriate services and meaningful support.

↘ Online research

📖 Ethical considerations

▼ Points to remember

- **Necessity and proportionality** - Consider why the work is necessary to help safeguard the online space, and how the proposed solution is proportional to the public safety threat in question
- **Social impact and Do No Harm** - Could what you produce be used in a way that creates harm? Are you acting in such a way that could expose others to content or material that they would otherwise not be viewing?
- **Human rights**
- **Inclusivity and diversity**
- **Data integrity**
- **Duty of care**
- **Transparency** - Do you share information across your teams in a transparent manner? Be careful to share what went well and more importantly what went wrong - so others can avoid these mistakes in the future.
- **Accountability** - What review structures are in place for your work, internal and/or external? How are you ensuring that lessons learned are swiftly captured and addressed?

Additional resources

[Moonshot's ethics framework](#)

'Setting your Moral Compass'

This workbook, particularly page 6, is a useful starting point for considering an ethical question or dilemma from different perspectives that may help in offering up insights or particular nuances that might not always be immediately obvious. It's most helpful in highlighting how there are generally not 'correct' answers, but different trade-offs in pursuing particular courses of action.

'The Responsible Open Source Investigations Workbook'

This guide, which can be copied to your Google drive and tailored to specific projects, is a really comprehensive resource for rigorously working through project and research stages.

↘ Research methodology

▼ Points to remember

📖 The OSINT process

- 1** Operational security - Make sure your digital footprint is not traceable
- 2** Setting objectives - What are the questions you would like to answer?
- 3** Research and scoping - To determine availability of data of interest as well as limitations
- 4** Identification - Triangulation techniques
- 5** Collection - Ongoing phase of data collection throughout a particular project
- 6** Analyze and process - Code, clean, translate, refine and analyse
- 7** Share - Prepare report / clear presentation of the findings and share securely

↘ The Five Ws of OSINT



Who

- Who is conducting the analysis?
- Who is the analysis about?



What

- What information is being sought?
- What was found?



Why

- Why is the analysis conducted?
- Why is the analysis important?



Where

- Where was the object of analysis found?



When

- Time/date stamp of activities?

Additional resources

[OSINT framework](#)

[Comprehensive list of OSINT tools](#)

[OSINT Techniques Resources](#)

[OSINT Techniques Chart](#)

Bellingcat [Online Investigation Toolkit](#)

Digital Security

▼ Points to remember

Example Digital Security Checklist

My laptop and workstation are secure:

- I have a privacy screen on my monitor.
- My home and/or office router passwords have been changed from the default.
- My laptop, charger, and laptop case are not labeled with my full name or any other links to me or my organization.
- I store my files in an approved secure location, ideally an encrypted cloud storage folder.
- I minimize paper documentation, and have a paper shredder for the secure disposal of printed sensitive information.

My devices cleared for work use are secure:

- Devices use a strong passcode, and I have fingerprint ID or Face ID enabled, if possible.
- I use only approved software, devices, and applications to fulfill my professional duties.
- Devices are encrypted.
- I use a VPN when connected to an unsecured network (e.g. public wifi).
- I have enabled multi-factor authentication for key accounts (e.g. email).
- I have provided an up to date list of all the devices - including personal - which I use to access organizational data.

I follow best practices for secure browsing:

- I use a secure password method, and avoid using personal details for passwords (e.g. pet names, place of birth).
- I do not have the same passwords across multiple accounts.
- I use a password manager.

My online presence:

- I've reviewed my online presence to identify risks.
- I've put security and privacy measures in place.
- I'm aware of the risk of phishing and doxing, and know how to report and respond to an incident internally.

I can navigate risk with my team:

- We have an organizational password policy.
- I understand the process for raising a security concern with a colleague or decision maker.
- I can work with my team to identify and implement mitigations, and understand how to review security incidents.
- I understand what the steps are to identify, report, and manage a digital security breach.
- I am aware that digital security is an ongoing and shared responsibility, and it is essential to know how to protect sensitive data and stay safe online.

Additional resources

Here are some of the tools we can recommend - it's not an exhaustive list, and new tools do come out frequently - but make sure you're getting advice from a credible, reputable source.

Secure communications apps

- [Signal Messenger](#)
- [WhatsApp](#)
- [Privnote](#) (temporary encrypted file sharing)

Anti-virus software

- [Avast](#)
- [Malwarebytes](#)
- [Bitdefender](#)

File/drive encryption

- [On a Mac](#)
- [For Windows](#)

Secure browsing

- [NordVPN](#) - VPN service that encrypts your internet connection and hides your IP address and location. This is a paid service, and one we recommend as an important organizational investment
- Other VPN options are [Windscribe](#) and [TunnelBear](#)
- [Privacy Badger](#) - browser extension that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at
- [uBlock Origin](#) - browser extension that blocks ads, trackers and unwanted content

Privacy screen

- You'll need to find the right option for your computer/device, but here's an [example](#)

Secure data storage

- [Cloud encryption via Google](#)
- [Cloud encryption via Microsoft](#)

↘ Securing your online accounts

Introduction

The purpose of this document is to make sure you all have access to some quick guidance on how to temporarily or permanently reduce your online presence - essentially, making social media accounts private, hibernating your LinkedIn account, etc.

Whether you maintain personal social media accounts, and what you share, is a personal choice - just make sure it's an informed choice.

Taking these steps with your personal accounts will always be subject to individual discretion, but as a general point, it's important and useful to be mindful of your online footprint. These guidelines have been adapted from security specialists at [Security Positive](#) to support people and groups who need to be mindful of their online security.

🔒 Password management

- Strong passwords that you don't reuse
Secure password generators available at [Diceware](#) and [Avast](#)
- Multi-factor authentication (see below)
- Use a password manager like [LastPass](#) to create and maintain strong passwords
- Change your passwords regularly (every 90 days), and immediately if you have reason to believe that someone else knows it.

🔒 Multi-factor authentication across your personal accounts

Specific instructions on 2FA for common services are presented below; check www.twofactorauth.org to see what other services are supported.

- Email ([Gmail](#), [Yahoo!](#), [Outlook](#))
- [Facebook](#)
- [Instagram](#)
- [Twitter](#)
- [LinkedIn](#)
- [Snapchat](#)
- [Youtube](#)
- [Whatsapp](#)
- [Signal](#)
- [Telegram](#)
- [iCloud](#)
- [Google Drive](#)
- [Dropbox](#)
- [Paypal](#) (see if any other online banking service is listed at www.twofactorauth.org)
- Website hosts, like [GoDaddy](#), [DreamHost](#), [BlueHost](#), and [RackSpace](#).

🔒 Security Settings by Platform

LinkedIn

- You can temporarily “[hibernate](#)” your account so that your profile can’t be viewed.
- This doesn’t remove it from the Google index - but clicking through goes to an error page.
- Note that you won’t be able to reactivate it for 24 hours after first hibernating the account.
- You can opt to show only your first name and initial of your last name

Instagram

- [Make your account private.](#)
- [Delete old posts](#) that appear publicly or that give away home address, phone number, email address, or other personally identifying information.
- [Disallow location tags or location information](#)
- [Disallow any connections from tagging you in photos without your permission](#)
- [Set up 2FA](#)

Youtube

- [Set up 2FA](#) (via your Google Account)
- [Make your YouTube Channel Private](#)
- [Delete old posts and videos](#) that appear publicly or give away your home address, phone number, email address, or other personally identifying information
- [Restrict Embedding](#)

Facebook

- [Set up 2FA.](#) Page or group management is done by individuals accounts. Make sure anyone with access to your pages or groups is using 2FA.
- Remove any admins who no longer need access to your pages. Manage access vigilantly. If you use your personal profile for public work, consider shifting it to a public Page.
- [Make your personal account private.](#)
- [Disallow friends from tag you personally](#) in photos, status updates, or locations.
- Set up an Facebook account-specific email account that you don’t use elsewhere.
- Get alerts when an unknown device logs into your account.
- [Disallow location tags or location information.](#)
- [Delete old posts](#) that appear publicly or that give away home address, phone number, email address, or other personally identifying information.

X

- [Set up 2FA](#). Make sure anyone with access to your pages or groups is using 2FA.
- Remove any admins who no longer need access to your pages. Manage access vigilantly.
- If you use your personal profile for public work, consider shifting it to a public Page.
- [Make your account private](#)
- Get alerts when an unknown device logs into your account.
- [Disallow location tags or location information](#)
- [Disallow any connections from tagging you in photos without your permission](#)
- [Delete old posts, tweets, images](#), that appear publicly or that give away home address, phone number, email address, or other personally identifying information.

Snapchat

- [Set up 2FA](#)
- Make your snapchat account [private](#)
- Delete old [Messages](#) and [Memories](#) on snapchat
- [Disallow location tags or location information](#)
- Follow Snapchat's privacy tips [here](#).

TikTok

- [Set up 2FA](#)
- [Make your account private](#)
- [Delete old posts](#) that appear publicly or that give away home address, phone number, email address, or other personally identifying information.
- [Change your location information](#) so it isn't your real information
- [Update your privacy controls](#)

Managing your online footprint

- Review the first 5-15 pages of search engine results for your name
 - Report content on Google products for removal [here](#)
 - Here is a [short primer](#) on making data deletion requests
- Keep a record of any sensitive content you find.
- Identify and delete forgotten social media accounts.
- Consider changing your name on accounts to an alias, or using a separate email.
- Receive alerts if your email address is in a data breach - sign up at [Have I been pwned?](#)

Staff Welfare

A few general principles

- 1** Risk minimization
- 2** Share and understand the burden
- 3** External support/ supervision
- 4** Clarity of roles and expectations
- 5** Vetting & recruitment
- 6** Lead by example/ culture of empathy

Community-inspired welfare practices

Some ideas that were shared during the training about how we can take care of ourselves and support each other as a team.

Personal wellbeing

- Stay hydrated, take walks, and allow time for power naps.
- Practice meditation, listen to music, dance, and take time off to decompress.
- Spend time with family and friends, and prioritize outdoor activities.
- Set boundaries: limit phone use during personal time and put social media on silent.
- Listen to your body: take breaks when needed and don't feel guilty for self-care.

Team wellbeing

- Hold regular debriefs, weekly check-ins, and provide counseling or therapy for the team.
- Offer team-building activities and paid time off, including an off day on birthdays.
- Create a safe environment that promotes freedom of expression and solidarity.
- Organize security trainings, ensure work-life balance, and schedule mandatory days off to avoid burnout.

Organizational practices

- Promote flexible hours and remote work.
- Encourage a culture of fun and relaxation with activities like Friday half days or naps.
- Learn about collective wellbeing and let go of guilt tied to productivity limits.

↘ Survivor-centered design

▼ Points to remember

📖 Five core design principles

1 Accessibility

The landing page needs to be accessible to all at-risk users with disabilities that affect online access including auditory, cognitive, neurological, physical, speech and visual disabilities. Moreover, accessibility also benefits people without disabilities, such as older people whose abilities change due to aging; people with ‘temporary disabilities’ such as a broken arm or missing spectacles; and people with situational limitations such as being in an environment where they cannot listen to audio.

The principles for making a website accessible go hand-in-hand with making the website clear, concise and easy to use. Some key considerations to make for physical disabilities include making buttons large and easily clickable, giving the user enough space to fill out a form and designing with mobile and touch screen in mind. Considerations for cognitive health disabilities include keeping users aware about next steps and timelines and explaining what will happen after completing a service.

2 Predictability

Five questions that a user needs to have answered when they arrive on a landing page:

- Where am I/what site is this?
- What is it for?
- Why should I be here and not on some other site?
- What can I find here?
- What can I do here?

3 Simplicity

- Improve legibility of the landing page
- Improve user’s first impressions
- Easier for the user to recognise the landing page for future visits
- Loads faster = better for low-bandwidth connections

4 Privacy and confidentiality

- Privacy policies and FAQs
- Direct acknowledgement of privacy concerns
- Non-intrusive user forms
- Consider users’ expectations of anonymity

5 Credibility

- Inspiring case studies
- Insights into case workers
- ‘About us’ pages
- Reference partner organizations

Contextual considerations



Communication

Delivery partners who provide intervention services should tailor the service provided to the local context. For example, if WhatsApp is the most popular messaging platform

In a country, then it makes sense to offer vulnerable users entry to a WhatsApp group in which they can speak to a counselor.

At the same time, Moonshot always recommends offering multiple methods of referral to allow for diverse circumstances and preferences.



Colour

The way we see and perceive colour is vastly impacted by a range of factors, including cultural context, our upbringing and personal preferences.



Images and symbols

Images and graphics should be chosen with care. This applies to imagery and symbols which could both be seen as supportive of a user’s point of view, or which could appear to be refuting it.



Text and copy

The tone of the landing page text should be open, clear and empathic.

Additional resources



Accessibility

The [Web Content Accessibility Guidelines \(WCAG\)](#) are a shared standard for web content accessibility for individuals, organizations and governments. They were created by the World Wide Web consortium, which runs specific working groups for accessibility. The [A11Y Project](#), a community-driven project for web accessibility and the [UK's Government Digital Service department](#), also share very useful accessibility checklists.

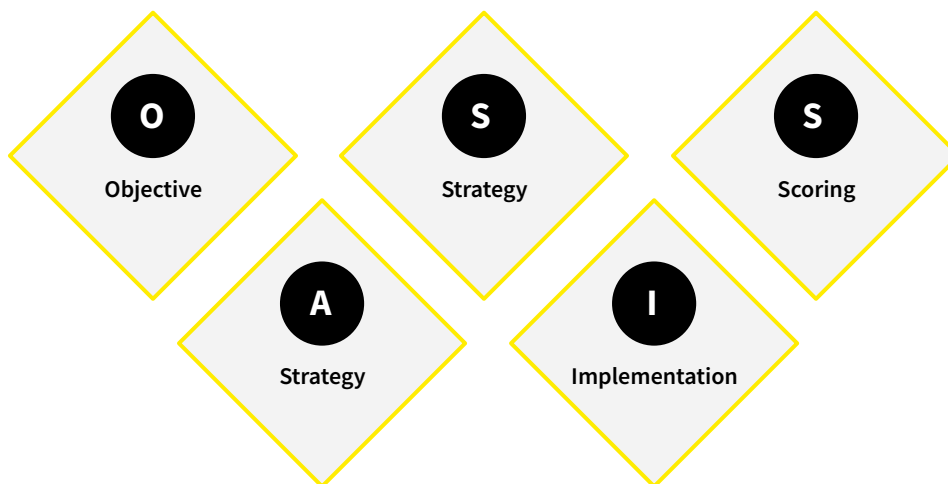
[One Click Accessibility](#) is a free plugin make WordPress websites accessible for people with disabilities.

↘ Digital campaigns

▼ Points to remember

- ▷ A digital communication campaign consists of setting up a communication campaign exclusively on digital platforms (e.g. social media, marketing tools such as Google Ads).
- ▷ Digital campaigns, particularly on social networks, can be used to combat TFGBV, hate speech and violent extremism online.
- ▷ To develop a digital campaign, it is important to consider the principles of strategic communication: define your problem and your audience, create the message you want to get across, choose your platforms, prepare a communication plan and a budget, and measure its impact. The OASIS framework is an important tool for planning digital campaigns.

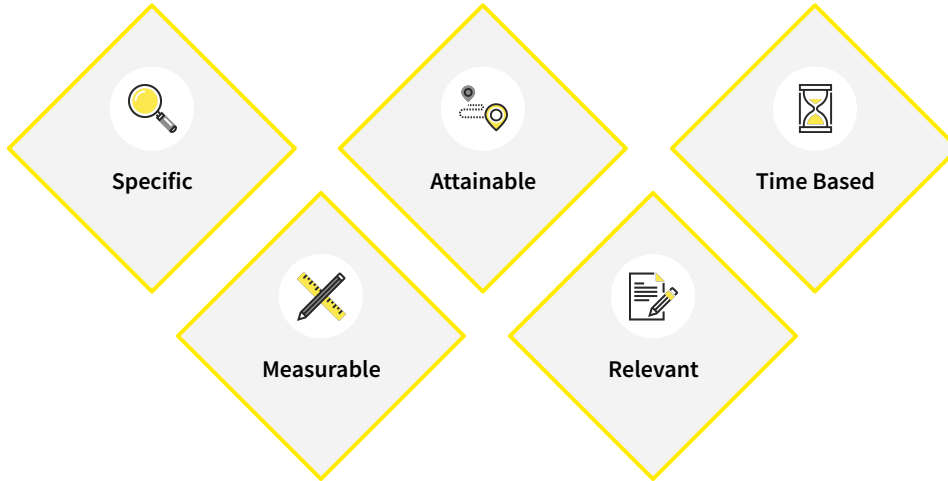
↘ Oasis campaign planning framework



Objective setting

- 1 Before planning the digital campaign, it's important to define the problem and the audience you want to address.
- 2 Defining the problem allows us to understand the theory of change of the digital campaign, as well as the objectives to be achieved.
 - The SMART rule is used to define specific, measurable, achievable, relevant and time-bound objectives for the digital campaign.

↳ SMART objectives are



Defining your audience

- 1** The target audience is the group of people you want to persuade with a targeted message. It is important to define the audience in order to create a relevant and convincing digital campaign and message.
 - Questions to ask when defining the target audience include their age, geographical location, language, vulnerabilities, interests and hobbies..
- 2** Empathy is an essential element in digital campaigns.

Campaign strategy and implementation

Choosing your platform

- Digital campaigns can be launched on a multitude of platforms, including social networks, search engines, messaging applications, and audio and video sharing platforms. Consider the following:
 - Where can you reach your audience?
 - What resources do you have?
 - Are there legal restrictions on certain platforms in your country?
 - What technical know-how do you need?
- Paid advertising on websites or search engines is also an effective way of quickly reaching your target audience in an accurate manner (using things like keyword targeting). However, it requires a fairly substantial financial and time investment.
- Manual distribution (content seeding) can also be used, i.e. manually placing links to your campaign content where they can be seen by your target audience.



Messenger

It is essential to choose a messenger for your campaign that is considered credible and influential by your target audience.



Branding

How will you present yourself in your campaign?

Will you use your organisation's social media profiles or create specific, perhaps anonymous social media channels?



Crafting your message

- The process of creating the main message of the digital campaign, and the way in which the message is presented, is called framing.
- To frame a message properly, you need to define the problem that the campaign wants to solve, as well as the target audience. Then you need to present the problem to the audience and propose a solution using simple, convincing and ethical language.
- Using emotions is an effective technique for creating convincing messages. You can use positive emotions such as joy and hope, or negative emotions such as fear and anger. Emotions can be conveyed through text, but also through images and music.



Call to action

A good digital campaign is clear about whether it wants to change what people do, or how they think about a specific issue. The former will have a clear call to action, whereas the latter will have more generic appeals.

Monitoring and evaluation

It sets out to answer the question: “*Did we achieve what we set out to do?*”

Monitoring is what you do while your campaign is running, while *Evaluation* is what you do at the end of the campaign to assess its overall performance.

In order to assess your campaign, you first need to **define how you're going to measure success**: how do you know that you have reached your objective? Where do you get this data from?

You should pay close attention to how your campaign is received by your target audience.



How much engagement do you get?



How many comments are users leaving?






Are these comments positive, negative or neutral?







Is your content being shared by a lot of users?

A lot of campaigns rely on platform metrics - e.g. number of clicks, impressions, website visits, number and nature of comments, etc. Campaigns that have a clear call to action can also include other metrics - e.g. if your campaign asks people to support a local initiative, you can count the number of people who have actually provided support as an evaluation metric. Or, if your campaign asks people to sign a petition, you could count the number of people who sign.

If you are unhappy with the level of engagement, you need to analyze why this is the case.

-  Are you posting your content at the wrong time? Maybe posting it at a time when your target audience is most active on the internet would be better?
-  Or is there something wrong with your campaign content? Maybe the message, its tone or presentation don't appeal to your target audience?
-  Maybe you are not reaching the right audience? Are the people that are looking at your content really the people you would like to reach?

Some of the most important questions to ask when evaluating your campaign performance are:

-  **1 Inputs**
What did you do before and during the campaign? What went into developing the campaign methodology and campaign content? What resources did you need?
-  **2 Outputs**
What did you do, make or produce, to help meet your objectives? Did you make a video or a campaign website, or series of cartoons?
-  **3 Outtakes**
What information/lessons were learned? Is there anything you would do differently next time?
-  **4 Outcomes**
What change has happened as a result of your campaign?



Additional resources

[How to create a Gantt chart](#)

[Sociallymap](#): Platform for automating the publication of content on different social networks. This can also be done manually through the platform.

[Google Ads Guide](#): Guide to how advertising works.

Free content creation resources

- Royalty-free images: [unsplash](#) or [freeimages](#)
- Royalty-free music: [Bensound](#)
- Icons: [flaticon](#)
- Sound editor and recorder (PC and Mac): [Audacity](#)
- Video editors (PC and Mac): [OpenShot](#)
- Design templates: [Canva](#)
- [Sociallymap](#): Platform for automating the publication of content on different social networks. This can also be done manually through the platform.
- [Google Ads Guide](#): Guide to how advertising works.

