Virtual Trainings Gate

A toolkit for safe and effective virtual Trainings

GPPAC
A Network of People
Building Peace

ندعاء العدالة
JUSTICECALL
Advocate for Justice and peace

Virtual Trainings Gate
A toolkit for safe and effective virtual Trainings

Justice Call
2021

Virtual Trainings Gate
A toolkit for safe and effective virtual Trainings

Issued by:
Justice Call

Editors:

Safa Harak
Peace & Civic Educator, and curriculum designer

Mahmoud Abdelzaher
Human Rights researcher and facilitator

Ayah Othman
Illustration and design

Watfa Shehade
Esra Saleh
English translation

 facebook.com/JusiceCall2030

 instagram.com/justicecallorg/?hl=en

 twitter.com/justiceCallOrg

 linkedin.com/company/justicecall/?viewAsMember=true

Content

Before we go...

About this toolkit

This toolkit attempts to provide a comprehensive practical knowledge framework for practitioners who work in the field of civic education and peacebuilding to help them continue their work and implement their training programs online in light of the current challenges imposed by the epidemiological spread situation of the emerging coronavirus. The guide provides technical alternatives that allow the implementation of workshops remotely and in an efficient and effective way, as well as suggestions of some basic training activities that could be integrated into any training program and to be framed to be provided online.

This toolkit is a step on the development way of the trainers of civic education and peacebuilding in the MENA region. Through the included tools and activities, the toolkit attempts to enhance the impact of these individuals, organizations, and initiatives where they are active, and guarantees their ability to continue their work in confronting the current challenges. Moreover, it encourages them to digitalize a part of their job permanently to overcome various challenges such as: the cost of implementation of on site training programs, difficulty to approach some areas, and the inability of some target groups to access the training programs that are organized on ground in a fair way.
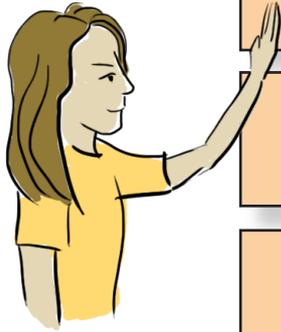
Why this toolkit?

Trainers face challenges regarding online civic education and peacebuilding training for many reasons, among which:

- The lack of experience in dealing with virtual platforms and tools on both sides (training staff and trainees).

- The misassumption that depending on getting together in one place for implementing a training program related to civic education, peacebuilding and life skills, is the only way to develop and gain skills. Therefore, the distant learning platforms are thought to be more suitable for programs based on knowledge and academic content, as if we are telling ourselves that online learning is only for imparting pre-established knowledge, and that gaining knowledge through experience should only be in the training room.

- Challenges associated with the devices used (an old/new smartphone or a computer - and the capabilities of each of them, the strength of the connection, the availability of the internet for financial reasons, etc.), which are difficult to predict when dealing with a diverse group of participants as in training and workshops.

This toolkit – partially- attempts to deal with these challenges in terms of lack of knowledge and skills with facilitating ways and tools via the internet, and seeks to be a station in the self-education and development path of each facilitator who is concerned with spreading a culture of peace or civic education.

The toolkit is divided into 3 main parts:

First part: discusses the most important platforms that could be used in implementation of training events remotely.

Second part: discusses the main practices for protection of digital security of internet users.

Third part: provides a various group of activities and tips to be integrated within any training program and could be used online.

How to use the toolkit?

We expect the trainers to improve their special activities in accordance with the examples and tips mentioned here.This toolkit is a way to how to use different platforms basically and includes examples of usual activities that are essential for the workshop (such as refresher games, discussion activities…). This toolkit is not considered a technical guide as known, as it does not list the technical details of all the tools and platforms mentioned. Rather it only provides the general framework for using these platforms, the purpose of their use, and the reasons for their preference over others.

We appreciate your Feedback!
Help us improve this toolkit with your brilliant ideas and recommendations by emailing us on info@justicecall.org or scan this code

Part one:
Essential tools for organizing and implementing online training

There is a package of digital tools that could be used in different steps of coordination and planning of a training event online; could be used before the event, normally a video communication platform will be needed to achieve. The following tools are recommended to arrange a more interactive digital planning, whether with the working team or the participants.
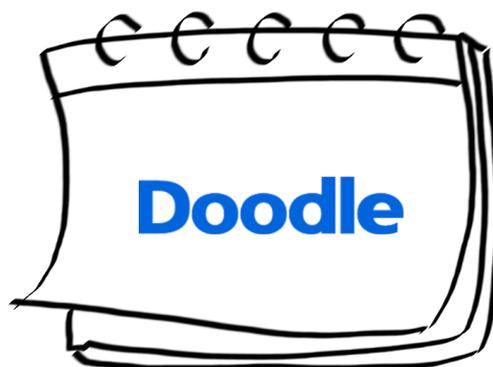
Doodle

The slogan of this platform is: It shouldn't take 30 emails to schedule a 30-minute meeting.
This slogan briefly explains the function of Doodle, as it helps you in polling the opinions of the participants in the workshop about the appropriate date for holding the event.
Through this platform, it is possible to determine the proposed dates for holding the workshop and send a voting link to the target groups via e-mail, WhatsApp or others. After the voting process is over, you can find out the date that suits the majority of the participants.
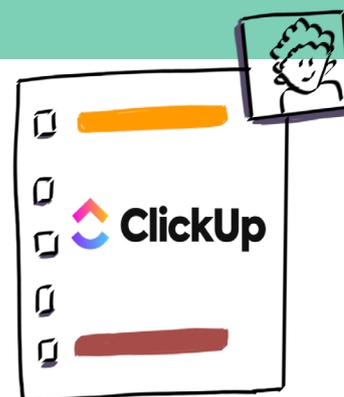Doodle provides the main services freely, and there are paid services with more features.
You can reach these services on: https://doodle.com/en

Clickup

This platform provides a remote project management service, which helps working teams in organizing and distributing tasks, as well as following the progress of work with each task. Speaking of which, this platform can be used by the team in charge of managing the event to distribute their tasks and follow up their completion by the team leader and the rest of the team members.

Mindmeister

This platform provides the service mind mapping for its users free of charge; a question can be asked to the team or even to potential participants in your workshop and they answer through the link of the mind map and enjoy a complex and attractive view of the answers of the rest of the team instead of the traditional image of collecting responses such as Google Docs services and others. This platform can be used before or during the workshop to implement activities and manage the brainstorming processes with the participants.

As for conducting the workshop itself, there are dozens of platforms that provide hosting video meetings. It is important to select a platform that suits the training needs, but generally, there are some factors that helps to choose one such as:

Worldwide, there are dozens of hosting platforms for online video conferences. Some of them are free and some are paid. The software required by each platform to get its services varies, especially via computers. Some platforms need to install programs on the operating system and others only need to open a new window on the internet browser. As for mobile phones, most of these platforms provide their services through an application that is downloaded from App stores, Such as Google Play for Android phones and Apple store for iOS phones.

In the following lines we will learn about the most important video conferencing service providers that can be selected to host workshops and training programs.
The most famous platforms for online workshops are:

Zoom

The most popular platform for online video meetings, conferences and learning sessions, as it is characterized by its easy use, the quality of video and audio, and various collaboration tools where hosts can share the screens of their phones and computers with the ability to comment and clarify with audio and typing.

The platform is suitable for many popular operating systems such as Android,
Windows, Mac, BlackBerry, IOS and others. Therefore, it is one of the best options for official online meetings, interviews and conferences.
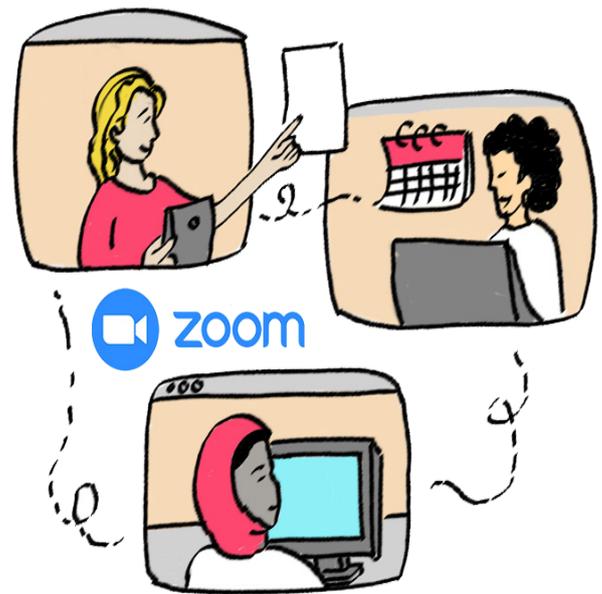
Moreover, Zoom allows the possibility of connecting a large number of people together, that may amount to 100 without affecting the quality of services provided and for free as well. The Zoom platform also features the ability to divide the participants into working groups, and the ability to record workshop sessions and save them to your computer. Unpaid accounts on Zoom allow video meetings of no more than 40 minutes, so they are not practical in long workshops unless you use the paid services.

Despite its many advantages, many digital security experts do not use this platform, especially after some technical researchers discovered security vulnerabilities in the application and program that could allow hackers to spy on the sessions, which prompted major companies to announce that they stopped using Zoom. However, the digital risks associated with using the Zoom platform can be reduced by following these steps:

- It is better not to share the meeting link on social media such as Facebook and Twitter pages. Rather, it can be sent to participants only.
- Don›t share a personal meeting ID. It is preferable to generate a random meeting ID.
- Use a password for the training event and share it only with the participants.
- Disable "the join before host" feature, which allows participants to join the event before the host joins.
- It is always preferred to use the "waiting room" feature, which is a space where participants join and wait for event organizers to let them into the main virtual room.
- It is important to disable "the screen sharing" feature for all participants and enable it only when needed.
- It can be useful to enable "the hosting sharing" feature and enable someone else to manage the event in case the main host suffers from any technical issues.
- It is important to disable "sharing files" feature and enable it only when needed.

The paid accounts on Zoom start at $149 per year, and there are multiple monthly payment options.

You can reach this service on: https://zoom.us/

Jitsi

It is an open source and free program that provides the ability of texting, audio and video calls, sharing files and screen sharing in a secure and easy way. In addition, Jitsi.org foundation also provides the Jitsi Meet on its website, which is a free, easy, safe way to use for audio and video calls via the browser. Therefore, it can be considered as an open source, free alternative to services such as Google Meet, Skype, Zoom and others.

In addition to the completely free services, Jitsi platform allows its users to conduct video meetings via an internet browser without the need to install any software on the operating system. For mobile phones, it is necessary to install the Jitsi free application. The platform offers its services with no restriction on the number of participants or the time of the activity/session. In addition, the platform works on most well-known operating systems, whether on computers or mobile phones.

Jitsi is the best choice if you need to hold a training program that is private and secure, and it is very difficult to hack its content, as all communications made through Jitsi are encrypted and there is no need to create an account or provide any personal data or information such as phone number, email address or any other information - which helps protect the privacy of users. Also, joining a Jitsi session only requires knowledge of the data of the session.

Jitsi allows its users to live stream the session via youtube as well as record and save it via DropBox or embed it on other websites.

A unique feature of Jitsi is that this platform allows you to join a session through a phone call without the need for internet, but this option should not be used with sensitive or confidential meetings, as the audio content of the session will be available by the telecommunication company that was used to make the call to join the session.

Despite the recent popularity of the Jitsi platform and its preference by a large number of internet experts, especially those interested in protecting privacy, it suffers from some technical problems that appear with holding large or medium-number meetings. Also, the platform does not provide some of the features offered by competing platforms such as dividing participants for subgroups.

You can reach this service on: https://jitsi.org/

Microsoft Teams

Microsoft Teams is a chat-based platform for collaboration, in addition to sharing documents, online meetings, and many more useful features for remote communication, especially between working teams.

The service can be used efficiently in distance training and learning programs, as this service has earned the trust of millions of users and official authorities since its launch in 2017.

Microsoft Teams allows the ability to share content with other Microsoft applications such as the Microsoft Office, and documents can be stored via Share-Point. Each team using Microsoft Teams provides a space in SharePoint Online. The service is available in more than 19 languages, including Arabic.

The service is primarily paid and included in the Office package. The service can also be purchased individually at a cost starting from $5 per user monthly.

You can reach this service on: https://www.microsoft.com/en-ww/microsoft-365/microsoft-teams/group-chat-software

There are dozens of other platforms that offer video meeting hosting services other than the above three models such as:

Part Two:

Basic practices for protection of digital security

With the increase in reliance on the Internet in our professional and personal lives, the possibilities of our exposure to risks and threats on the internet that threaten not only our digital existence, but also directly affect our personal security. In this part, we will be briefly introduced to a group of essential tools and practices to keep the digital security of NGOs, and how to protect the data of those who involved in their activities in general, and in online training activities in particular.

Six main rules to work securely while organizing online training activities:

1- Building capacity on internet usage

There are no programs that are capable of your protection of all the threats and malware. Your knowledge of these programs, how they are used, and your behavior online is far more important than the availability of the software itself. Stay informed of updates issued by governments, anti-malware companies, and digital security experts, and avoid using any program if it is found to have vulnerabilities.

2- The weak spot is the most important

"The strength of a chain is measured by the strength of its weakest link". This applies to digital security as well; as the security strength of all the organization's digital transactions is measured by the strength of its weakest components. Therefore, one employee who acts recklessly over the internet may threaten the whole organization's website and its effectiveness, as well as during the training activities. One participant could threaten the data of all the participants, like what happened during the use of the ZOOM program in the United States when one of the participants shared the meeting data via Facebook, and the meeting was hacked by that information.

3- High cost does not mean high security

Do not assume that the security solutions of high cost are the best; if you bought the most expensive anti-virus in the world, and hand it to employees who are not trained to use it, then you have spent money in vain. Attention should be paid to integrated solutions to secure the digital presence and activity of the organization. Also, if you use an expensive platform, it does not mean that it will provide you with the highest degree of security.

4- Do not trust anyone online

Computer security tips seem like you should never trust anyone but yourself. In the real world, you should almost certainly trust a lot of people with at least some of your information, from your close family members or friends to your doctor or lawyer. But in the digital space, it's hard to understand who and what to trust. Always keep passwords and information that affect the digital security of your organization away from sharing with anyone. And remember, when you share the secret with a smaller number of people, the better the chance that it will remain a secret. Always make sure that the data of the workshops and dialogue activities you organize are not shared with non-target people.

5-Full online security is not possible. Always there are compromises

Set security policies that suit your organization's work, activities, risks, and the implementation steps you will take, as well as your colleagues. Any theoretically perfect security policy will not work if it is hard to be implemented on daily basis. For example, you may prefer to use Zoom as it provides many good features for an interactive event, although Zoom does not provide sufficient security for the participants' data. On the other hand, you may prefer to use the Jitsi platform because it provides a better degree of security, although it may not offer the same features as ZOOM.

6- Today's security won't last forever

Digital security experts continuously reveal security problems and vulnerabilities in various operating systems, programs, and applications. You have to be updated with this news and stop using any program that appears to have security vulnerabilities until its owner company fixes them. Always remember that using a program on your device because it is safe last year or week, does not mean it is still safe now.

Malware:

It is small but harmful software, transmitted to your computers via suspicious websites, or using a USB memory that is not safely guaranteed.

Symptoms of malware vary from one to another, but in general, they all slow down the operating system, annoy users with advertisement windows, and leak personal information from their device.

Malware stands for «Malicious Software» and it is a software that is intentionally inserted into a computer for malicious purposes, without the user›s consent. This software aims to completely or partially disable the computer, collect sensitive information, or access user files.

Once a malware is installed, the difficulty of its removal will depend on its severity and action, ranging from a minor annoyance (the appearance of some unwanted advertising windows) to an irreparable harm that requires reformatting of the hard drive for example.

Spyware:

They are programs that are surreptitiously installed on computers to spy on users or take partial control of the computer, without the user›s knowledge. While the name (spyware) refers to secret programs that monitor users› behavior, their tasks go far beyond mere monitoring. Spyware can collect various personal information, such as web browsing, and monitor visited websites.

They can also take over the infected computer, control it and perform several tasks, such as: installing additional programs, transferring advertising revenue to third parties, changing the web browser's home page, redirecting the web browser, redirecting malicious and harmful websites that would cause more viruses. Spyware also can change the computer's settings, leading to its slow down and affecting the internet connection.

Cryptojacking:

Cryptojacking, or unauthorized mining of encrypted digital currency, is the process of hijacking the victim's device without his knowledge and exploiting its computational capabilities to mine cryptocurrencies. To achieve this, attackers usually either use social engineering methods such as sending malicious links to the victims that infect the device with cryptocurrency mining software, or through infecting a website with a mining software, so that the mining takes place via the browser on the devices of the infected website visitors.

Either way, the mining software will run automatically while the computer is in use, often without anyone noticing the infection. Unlike the majority of malware that infects devices, unauthorized mining software does not harm the victim›s data, information, operating system, or internet connection. Rather they steal processing capabilities from the CPU or GPU.

This lowers device performance, which can be a minor inconvenience for users of the infected devices, and there will be a rise in the electricity bill on long term, because of the electricity used to feed the processor involved in performing the necessary calculations for mining. In case that a company or organization's computer has been infected, this will lead to a reduction in the performance of all infected devices, and consequently the performance of employees / employees, as well as an increase in the electricity bill. Also, because the devices heat up when they are constantly performing the mining calculations, this increases the possibility of the CPU or cooling fans to fail in the long run.

Financial profit is the main objective of this attack. What is mined on the victims' devices of encrypted digital money, will go to the attacker's account, who can later use this money as wished, such as converting it into (traditional) cash or using the digital currency to purchase assets, goods and services.
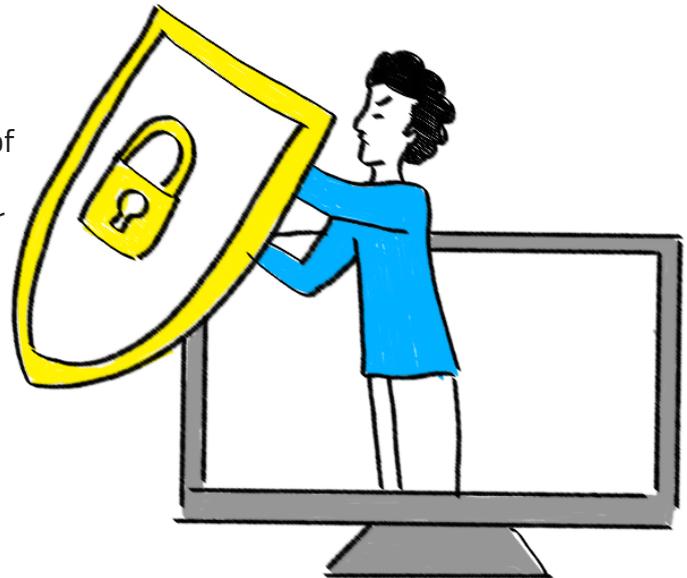
Social engineering:

The use of the attacker's information about the victims to deceive them so that they voluntarily reveal confidential information or give the attacker the opportunity to gain access to confidential information. Or the victim does something he wouldn›t have done if not deceived by the attacker.

Social engineering methods do not need deep technical knowledge so anyone with a certain amount of savvy can perform social engineering attacks.

Confronting digital risks

1- Stop using pirated software:

It is impossible to rely on pirated copies of the operating systems or essential software on your computer without threatening the digital security of your organization and your team. Pirated versions contain built-in malware, security vulnerabilities, or both. In case that you cannot purchase a program, you will have to put some effort into looking for a free alternative. "Alternativeto" website helps you find free alternatives to paid programs and recommend them to choose from. You can visit the website on: https://alternativeto.net.
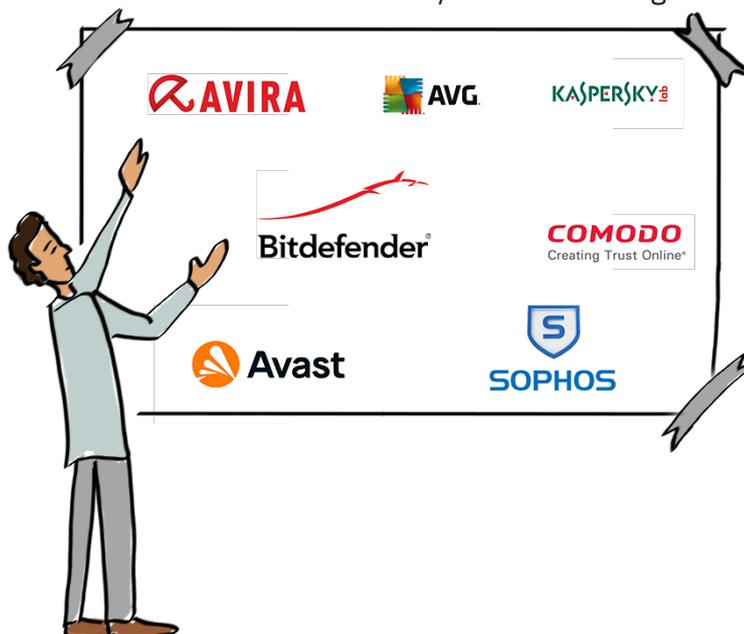
2-Update all the software you use:

Via the mobile phone and the computer, make sure that the operating systems you use, and all the programs and applications installed are updated on a daily basis. The companies that own this software usually launch updates about discovering security vulnerabilities in one of their products. Making sure that these products remain updated ensures that you fix these vulnerabilities quickly before they can harm you. This point is also related to the first point, as pirated software usually cannot receive new updates, and this is another reason to use legitimate copies of this software.

3-Always use an updated antivirus:

If you are a Windows user, you need to install a special program for protection against viruses and other malware. Most of the antiviruses worldwide offer free versions with fewer features, but they do the job of defending the device against malware, you just have to make sure to keep it up to date. You can choose between the free versions available from any of the following antiviruses:

The free versions of these programs do not provide full security as the paid ones. Therefore, it is necessary to use a separate program to protect against malware and spyware that traditional antiviruses could not succeed in dealing with. In this context, we recommend "Malwarebytes", which has a free version as well.

4- Use a strong password for your account:

You should carefully choose the passwords for your various accounts on the internet, whether for personal or professional accounts. Good passwords are characterized with:
- **Longer > 14 characters**
- **Memorable.**
- **Complex (uppercase and lowercase letters, numbers and symbols).**
- **Non-duplicate.**
- **Non-sequential (such as choosing FGH12 as a password for Facebook and FGH13 for Twitter).**
- **Non-personal (does not contain name, phone number, date of birth...etc).**
- **Confidential.**

Some websites allow you to choose a password of a number of words instead of a single word. You can also choose very complex passwords and save them in a one of the programs known as password vaults. In any case, never write down the password on a paper in your notebook or a file on your computer.

5- Be careful when using the internet:

Your digital awareness is your first line of defense against digital threats. You have to be careful in dealing with messages that contain links, even if the source of the message is known to you. You should also stay away from suspicious websites that ask you to download files on your device or visit unnecessary external links.
If you suspected a link sent to you through an email or otherwise, you can check it using the VirusTotal service before opening it. Just copy and paste the link on the website and it will scan it with dozens of antiviruses programs and show you the result. The same website can scan suspicious files by downloading them from a device before you start to open and use them.
This service can be used via the link: https://www.virustotal.com

6-Activate the two-step verification feature:

Currently, most of the major websites offer 2-step verification as an additional feature to secure accounts. When activating this feature, the user must verify his identity through two steps of security. This procedure requires a combination of username/password as well as a security code that is sent to the user via a mobile phone or other media.
This feature protects personal accounts from hacking and theft. Once, the account is hacked, the hacker will ban you from your account. Enabling 2-Step Verification will prevent the attacker from accessing your account even if they have your username and password. You will be notified of a failed attempt to log in to your account.

Improving privacy settings when using the internet

Some operating systems preserve the users' privacy to a great extent and some do not. Unfortunately, the popular operating systems, whether for computers or mobile phones, belong to the second type. In favor of the owning companies, these systems collect an enormous amount of data about users, their behaviors, and lives, save these data and sell them to third parties that may use them to manipulate the lives of millions of people. In the next part, we will know about some useful tips to enhance the privacy of users while dealing with some common operating systems and software.

Improving privacy when using Windows:

Despite being the most popular and widespread in the world, the Windows operating system, unfortunately, has a bad repu-tation for maintaining the privacy of users, so some settings can be modified within the operating system to enjoy a higher level of privacy while using this system. In general, it is important to:

- Disable advertising ID:

Advertising ID (Identifier) is one of the most important privacy setting that should be disabled, as this identifier is fully integrated into all advertising settings of Windows and third parties collaborating with Microsoft.

Each Windows 10 user has an advertising ID that allows Microsoft to collect information about them to create a «profile» that can be used by advertising agencies to display personalized ads that appear in apps and sometimes even the start menu.

To prevent Windows 10 from creating a personal profile about you, go to Settings and click on Privacy, then from the General menu, turn off the "Let apps use advertising ID" option.

- Disable location tracking:

It is also important to turn off the location feature because not only does Microsoft have access to this information, but third-party apps can also access your location data.

When you use Windows 10, it tracks your exact location and stores your location history in your account. To disable this feature, go to "Settings" and then click on "Privacy" then "Location" and disable "Location Services".

Windows 10 also gives you more control over the location settings for each app you have on the device, which means you can allow some apps to track your location and block others, and through the same menu you can clear the list of locations you've visited before.

- Disable access to the camera and microphone:

This is one of the most important privacy options that must be taken into account and can be controlled by going to "Settings" then "Privacy" and then to the "Camera" and "Microphone" settings, where the built-in webcam and microphone can be completely disabled at the system level.

However, it makes sense that some of the apps could access the camera and microphone, so it is rec-ommended to disable or enable the camera for each application separately.

Improving privacy when using Google services:

Currently, Google offers a great variety of services to its users, so that anyone who uses the internet in the modern world may find it difficult to try not to use these services provided and using alternatives to avoid the tracking and huge data collection that the company runs against users. However, some measures can be taken to ensure more privacy while using Google services, including the famous internet browser Google Chrome.

- The privacy setting for your Google account can be accessed by clicking on your profile picture at the top of your personal account page and then selecting the "Data & personalization" menu.
- By clicking on "Activity controls", the page of information that Google saved about your activity in the services and applications it provides will appear.
- It is recommended to disable "Web & App Activity" if you do not want your activity to be tracked and saved on Google websites, or within Google applications. Such as searches, or what apps have been downloaded, or search history within Google Maps and more.
- It is preferable to deactivate "Location History" if you do not want your location history to be saved. The Google Maps application installed on your devices records and archives your geographical location and movements.
- You can deactivate "Device's Information", if you do not want information about your device to be saved in your account which is linked to Google, and the information includes: contacts, installed applications, other information about the device ID and others.
- You can deactivate Youtube search history if you do not want your search history within the YouTube application or website to be saved. It is also possible to deactivate the YouTube watch history if you do not want the last videos you watched on YouTube to be saved.
- From the «Data & personalization» menu, you can go to the «Ad personalization» section and then go to Ads settings to turn off the customization of ads, if you would like not to display ads based on your activity on Google and its services, such as search history, geographic location, etc.

You can find how to apply these steps in the following video: https://www.youtube.com/watch?v=5S6x-pnVAmfo

Improving privacy when using Firefox internet browser:

- Through the preferences menu, you can access network settings and activate the DNS feature via HTTPS, which raises the level of privacy by encrypting the data of the DNS and helps protect against digital attacks such as Man in the Middle Attack.
- Through the «Privacy and Security» section of the browser, it is recommended to activate the enhanced tracking protection feature and set it to the hard level. It is the feature that blocks content that tries to track us when we visit websites, such as: trackers or cookies. Enabling this feature may cause some websites to be completely blocked, but it guarantees a higher degree of security.
- Through the "Privacy and Security" section, it is recommended to activate the "Do not track" feature and set it to permanent. This option activates sending a do-not-track request for all the websites we visit, and sending a request does not mean blocking trackers, so the website can ignore this request, but your request will be respected in case of websites that have good policies to protect users› privacy.

- It is recommended to use a master password for the browser. This feature adds a new layer of protection to passwords and usernames saved within the browser itself. If you requested to see a list of your saved passwords on your browser, you must enter your master password first.
- You can enjoy more privacy by using the "Private Browsing" Mode, which ensures that the browser does not record any data about the websites you enter when you activate a private browsing window (Incognito Window). The browser can be set so that it always works fully in private browsing mode by going to the Privacy and Security menu and activate the «Always use private browsing mode» option.
- It is recommended not to give the browser access to the camera or microphone, except when needed.
- Firefox collects and uses our search and usage data in studies of users and how they interact with websites or advertising campaigns. Firefox may share this information with other companies. Hence, it is recommended to disable the options of this feature from the «Privacy and Security» menu in the settings.

You can find how to apply these steps in the following video: https://www.youtube.com/watch?v=1Jyhoc51w9s. It is also generally recommended that you improve your default privacy settings on social media and other platforms that is regularly used. Tips to improve privacy can be found on each platform through traditional search engines.

Part Three:
Training activities

How to design a remote workshop or training?

1) Why?

The first step is to ask *why the training is carried out online?* A precautionary reason to keep the group safe? Because the participants are from different geographical areas and it is difficult to go to the place of implementing the training? To save cost? To allow more trainees? Or Because there are special needs of some participants that may be met by remote training and difficult to meet in the training room? Answering these questions, can help to chart the design for the training.

Example 1: I will implement the workshop remotely because it is part of a project that targets university students, and one of the project's objectives is to strengthen their technical competencies. Therefore, when designing activities, I will intentionally use a variety of tools and encourage them to make every effort to enable them to do so.

Example 2: I will implement the workshop remotely because some of the participants are from marginalized areas and will not be able to travel to the equipped training room. Therefore, I take care not to burden them with a lot of websites and tools that may not fit their mobile phones, and my goal becomes to carry out activities with the least capabilities.

The second step is to define the objectives of the workshop or training; the learning and educational objectives.

Completing the track of each of the above examples or others leads to the selection of the appropriate presentation and interaction method, tools, and duration of the training/workshop.

We always remember that the implementation of activities is not the objective. Rather, the activity is just a means to reach the planned objectives. Therefore, if we want to implement an online workshop for the first time, instead of asking "how to implement the same activity via the internet," we better ask about "how to achieve educational objectives with remote learning tools?" This means designing a new activity, or using a different methodology that includes some steps from the usual activity and some from another... and so on.

The result may seem the same in both cases, but in fact, we find that the extent of innovation and creativity in implementing workshops and training programs remotely to achieve educational objectives, is greater than adherence to the usual activities and only making modifications to them.

2) Complete the usual design steps

When implementing any training program, we ask the following questions:

- Why? (objectives)
- To whom? (participants)
- When? (Morning or evening, holiday or school/work day...etc)
- Where? (Main platform, participants' geographical locations)
- What? (Detailed content, workshop program)
- How? (Content delivery method)

As you can see, "how" comes at the last step and not at the beginning. In order to reach an innovative and appropriate methods for the new forms of online training, we must choose the "how" according to all the previous data after carefully reviewing them.

> If you are a trainer who is conducting an online workshop for the first time, it is recommended to read the toolkit, review the information mentioned on the different platforms and tools first, and design the training program later.

3) Considering peacebuilding when designing and implementing the workshop:

Sensitivity to the situation/context of the participants: If the trainers' culture or background differs from the group, they should ask some questions such as: *How will I be noticed (as an outsider)? What sensitive issues should I be aware of? What are the current tensions?*
Awareness of the cultural sensitivity can lead to understanding the unwillingness of some participants to switch on their camera during the session, for example, or the unwillingness of some (male or female) to do so also due to the economic class and house situation issues, which they do not want to share with everyone.

Vigilance and alertness: We mean 100% mental alertness during the session, even if the training task is distributed to a team of several trainers, especially when implementing a remote workshop, we recommend not to make it easy to leave and only participate in the trainer's time. This is to note everything about the group and their interaction. This will make all the difference to the group if they feel your presence with them and this will set an example of reciprocity during the session.
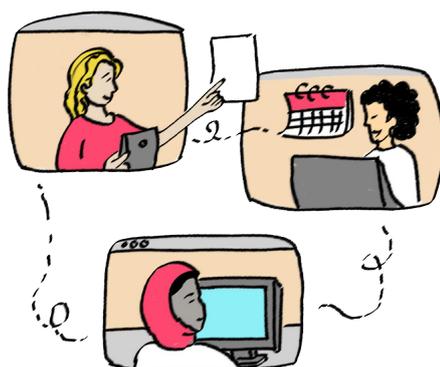
Active Listening: In addition to the importance of active listening in civic education and peacebuilding programs, during the implementation of a remote workshop, a greater effort must be put in; For example, paying attention to each other's attempts to speak at the same time, or comments written in the chat box.

Keeping balance and openness to participants evaluation notes: Ensuring the right balance between trust in the program and awareness of time management and the needs of the whole group; Some may need more time to participate while some may feel the need to move to the next session or need a break.

Inclusion and diversity: The principle of inclusion have to be taken into account; thinking about how to include marginalized groups or who may face difficulty in participating due to the imbalance of power and privileges compared to the rest of the group (males/females, people with disabilities, etc.). Ensuring that participants have equal opportunities to be part of the discussion. Examples of questions for the training team:
- Who talks the most in the group?
- Is there a gender balance in the training team?
- Are the tasks presented appropriately for the group according to their abilities (in the case of a blind participant, for example)?

Source- Adapted from: The «Youth and Peace» training suitcase issued by the Youth Without Borders Organization for Development.

Examples of activities

Icebreaking and refreshing

Among dozens of icebreaking activities carried out in the training rooms, some can be used in online training with some minor adjustments to suit the new situation. For example:

▪ My Item and something belong to me:

In this exercise, usually participants are asked to pick an adjective or an object that begins with the first letter of their name, provided that what they choose expresses or relates to them. For example: My name is Mona and I choose Mandarin because I like it so much. My name is Bassem and I choose Bell because I work in a school. And so on.

In an online workshop, the participant is requested to look for an object at home that starts with their initial. Hence, the participants move around their homes 1-3 minutes looking for the object and come back to the session and open the camera, then start to introduce themselves with the object they have found.

Ideas for updating the activity: You can add criteria for the chosen object such as being from a specific place in the house (kitchen, bedroom...), ask the participants to tell a story about that object, or do a cut and paste activity.

▪ Cut and paste:

After the participants have searched for an object in their homes with the object's name beginning with their initial, the first participant is requested to: Tell the group a sentence consisting of the participant›s name + an activity related to the object. For example: My name is Mona and I am slipping on the Mandarin's peel. Then the second participant should come up with a new sentence with his/her name and an activity related to the object based on the last sentence. For example: My name is Bassem and I am ringing the bell to talk about Mona slipping on the Mandarin's peel. The next participant would say: My name is Mohsen and I buy Bassem's bell with this money... and so on.

▪ Art time:

Sending a private message to the participants individually (send to xx instead of send to everyone) that includes a name of someone of the group. For example: sending Mona's name to Bassem, and Bassem's to Mohsen, and so on. Then they will be asked to draw a picture of the name owner through the Whiteboard tool, everyone participates in drawing and by the end the participants will try to guess pictures.

Source - Adapted from: Article 20 Online Refresher Games for Remote Meetings.

Code of Conduct:

Everybody is happy except me:

The participants are asked to bring a paper and pen, then they will have to imagine a situation in the future where everybody is going to be happy except for them. They will write down 10 reasons for that on half of the paper, on condition that these 10 reasons are directly related to them.
For example: "Many things have distracted me" turns to "I let many things distract me".
After listing the reasons, they will have to create another list in the other half of the paper, where they will change all the first list's points to better ones.
For example: "I arranged my time and priorities in order to pay a good attention during the training".
They will share 1 or 2 of the tips they wrote with the group. All tips will be written on a blank slide collectively by the participants themselves (on the whiteboard tool), or by the trainers through sharing screen, under the title: "Group's code of conduct".

Source - Adapted from: Civic Education Manual, by Goethe institute.

Tools that could be used for the final list:

- PowerPoint: prepare a slide presentation equipped with the title «Group's code of conduct « with the choice of an attractive design, and then add the tips of the participants within the prepared design.
- Google forms or a similar tool: then trainers display the results to save time.
- Miro, padlet, draw.io, whiteboard.fi, Jamboard: all are alternative websites for whiteboard to enable the group to write their ideas collectively and engagingly.

Expectations and fears:

Expectations and fears can be collected in a simple way by assigning participants to working groups in separate breakout rooms. Each team's task is to discuss their expectations and their concerns for the training.
Each team writes down their ideas before the deadline (10-15 minutes), and then will present them to the group when the separate rooms are closed.
The trainers' role is to lead a dialogue about expectations and fears to elicit appropriate working rules, which are written down and presented.
Tools that can be used for workgroups:
Google slides: Prepare a number of slides equal to the number of workgroups, each with a space designed for expectations and one for fears. Slides are numbered and renamed to help groups write in them.
Miro or similar platform: Set up one board for everyone and assign separate tables to each group/team.
It is enough for a team member to write down expectations and fears in the group chat box after returning to the main group - in case it is not possible to use external websites for technical or organizational reasons.

Training/ workshop program:

To present the workshop program, one of the following methods can be used:

- Design a table on a presentation program such as PowerPoint and share the screen while viewing it.
- Share the program in advance with the group via e-mail.
- A creative video can be made and shared with the group during the session or sent in advance using platforms such as moovly.com, renderforest.com, animaker.com or powtoon.com.

(Example of creating a video that can be used to display training content)

Discussion activities:

For an effective online discussion with a large group of participants, we recommend the following:
Split the participants into small working groups (5-10 people) to provide opportunities for all to participate.

- Allow an appropriate time for discussion based on the desired educational objectives of the activity; If the goal is only to develop dialogue skills, 15-20 minutes may be enough to hear different points of view and practice effective communication skills. While, if the topic of the discussion is of equal importance, a longer time may be needed (for example: at least 30 minutes for each dialogue sentence).
- It may be useful to delegate the tasks of "moderation" + "time monitoring" to one of the participants - if the person in charge of the workshop is not able to be present in the groups completely.
- It may be useful to assign the task of "recording the main ideas" to one of the participants and then present them to the whole group.
- To help the group have a structured conversation, the talking piece can be useful in many ways: for example, everyone but the speaker turns off the video camera, or agree to use a signal from who is available on the communication platform (such as the raised hand in Zoom).
- It is possible to ignore simultaneous training and use an alternative platform where the dialogue takes place by writing comments and responses to different ideas or supporting them using the "like" mark. this way could be sought for a number of reasons; Lack of time, lack of technical resources, which in turn hinders the group (or some individuals) from effectively participating through audio/video meeting programs, due to the importance of the topic of dialogue, which may extend the discussion period for more than a day during which the participants need to seek help from external sources or readings.
- In case of large number of participants, they can rewrite their names on the audio/video meeting program (such as Zoom) and add a unique code to each group; For example, adding number 1 next to the name of the participants in the separate room number «1» = Mona 1, Bassem 1.....etc.

Brainstorming and group planning:

There are many available digital tools that could be of more interest than traditional brainstorming sessions within the training room. But to ensure the efficacy of the used tool and its suitability for the group we recommend:

- knowing the type of devices used by the participants in advance, as some tools work only on a computer and cannot be used on a mobile phone, platforms usually require you to download an application to use the tool on the mobile phone. Also, the type and storage capacity of the device helps explain the possibility of downloading additional applications.
- Try any tool or platform in advance and perform all the steps as if you were a participant (using a computer + phone), in order to answer the following questions: Do I need to be logged in before participating or not? Is it required to take some steps before reaching the desired page? Download speed? Ease of navigation between the audio/video meeting program and the new website? etc.
- In the case of limited technical resources, a number of participants with the required capabilities are chosen to be representatives of their colleagues in small working groups. For example, the participant displays his/her screen and uses the platform to write what his/her colleagues tell them. Or the trainers perform that task and then require the participants to write their thoughts into the chat box.
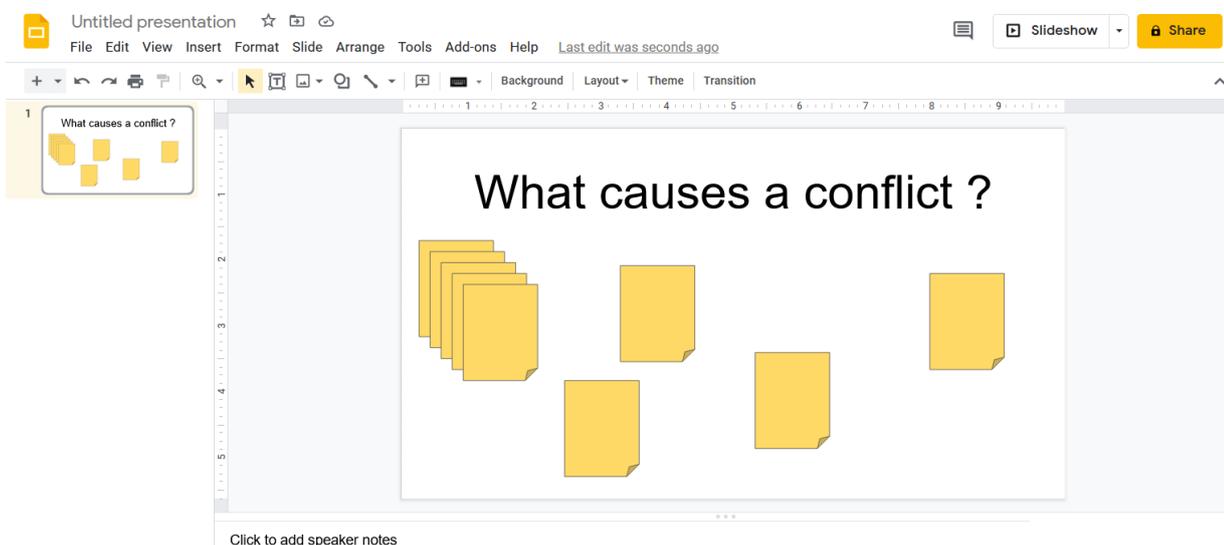
We prepare the participants for the next step by explaining and presenting the required task well, then we attach a link of the group brainstorming tool, with agreement on a specific duration for the task. Everyone should return to the video meeting program after (15 minutes for example).
In case of group planning, we continue the audio discussion on the meeting platform while putting our ideas on the planning platform.
When getting back to the group, we present the results and discuss the outputs. The process of brainstorming or planning may take several levels to reach the end objective. We prepare in advance the number of slides that are appropriate for all stages.
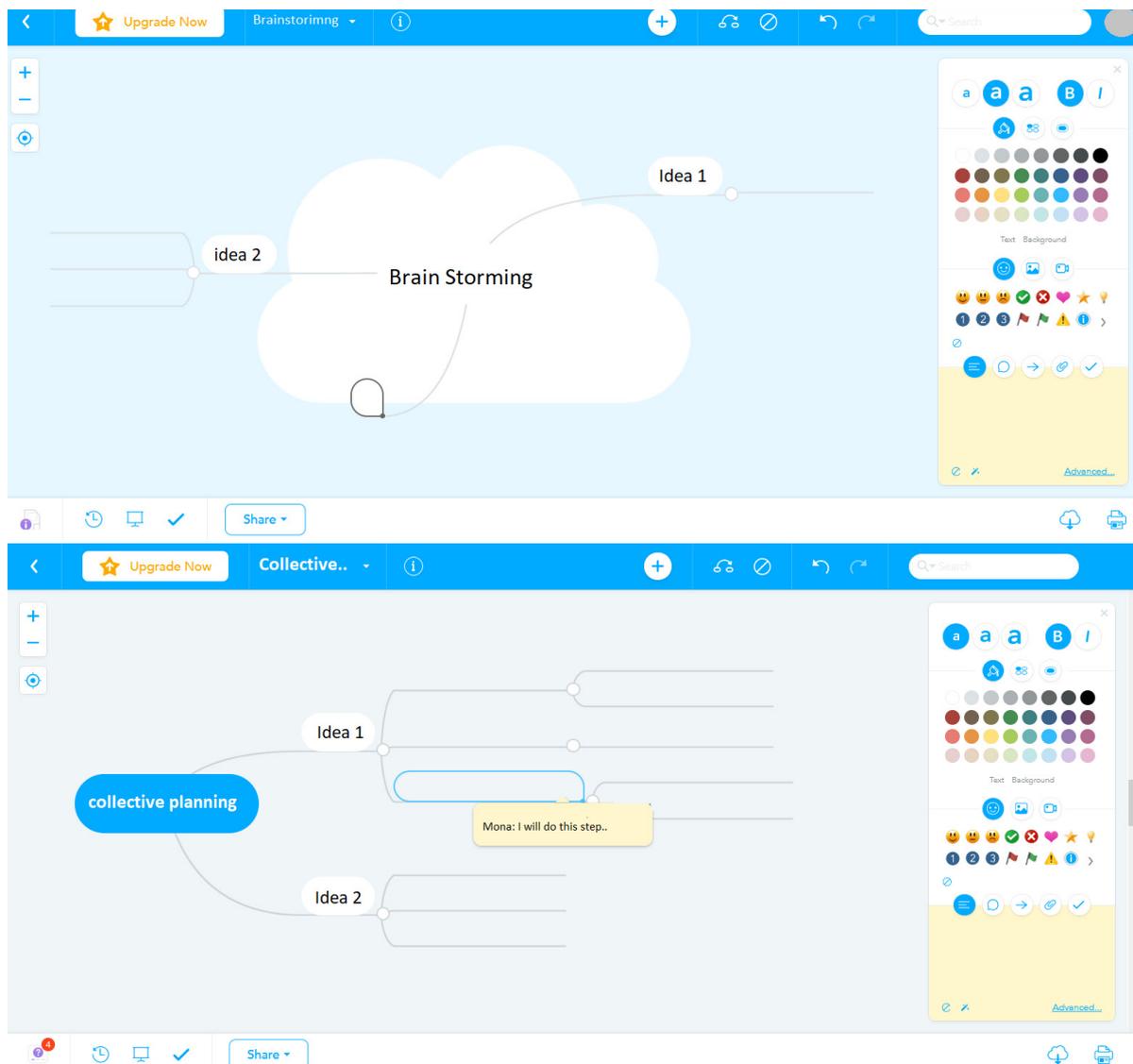**Examples of tools and platforms for brainstorming or group planning:**

- Sharing a pre-made link to **google slides,** designing the headlines you want to think about, or using sticky notes that participants use and move under the intended title. Google tools are free and available to everyone. It may require a big space for storage on the mobile phone when you need to download the application.

- **MindMeister,** requires logging in via email on the website first, and if using a mobile phone, you have to download its application, otherwise participants will not be able to interact and will only see what others write.

The website is characterized by its attractive designs and many capabilities. It also allows the design of 3 free boards simultaneously.

- **Miro website** can be used as an alternative. It provides additional features related to design, control of participants, various interaction tools on the board, and enables the group to dispense with the meeting program (for example, Zoom) and use communication features such as chat (for free) or make a video call on the same website (for a monthly payment)! It is recommended in group planning.

Role playing:

Through a video meeting program (such as Zoom), you can easily create role-play exercises using the following steps:

- Prepare in advance separate scripts for the roles of the activity.
- Send roles to the concerned participants via private message and ask everyone to go through their roles silently. In case of inquiries, participants can send their queries the same way to trainers.
- After making sure that the roles are clear to everyone, show the group scenario on the screen, then divide the participants into working groups that include different characters.
- If the stories for each group are different, Divide the groups first and send the stories via email or social media (Facebook messages for example).
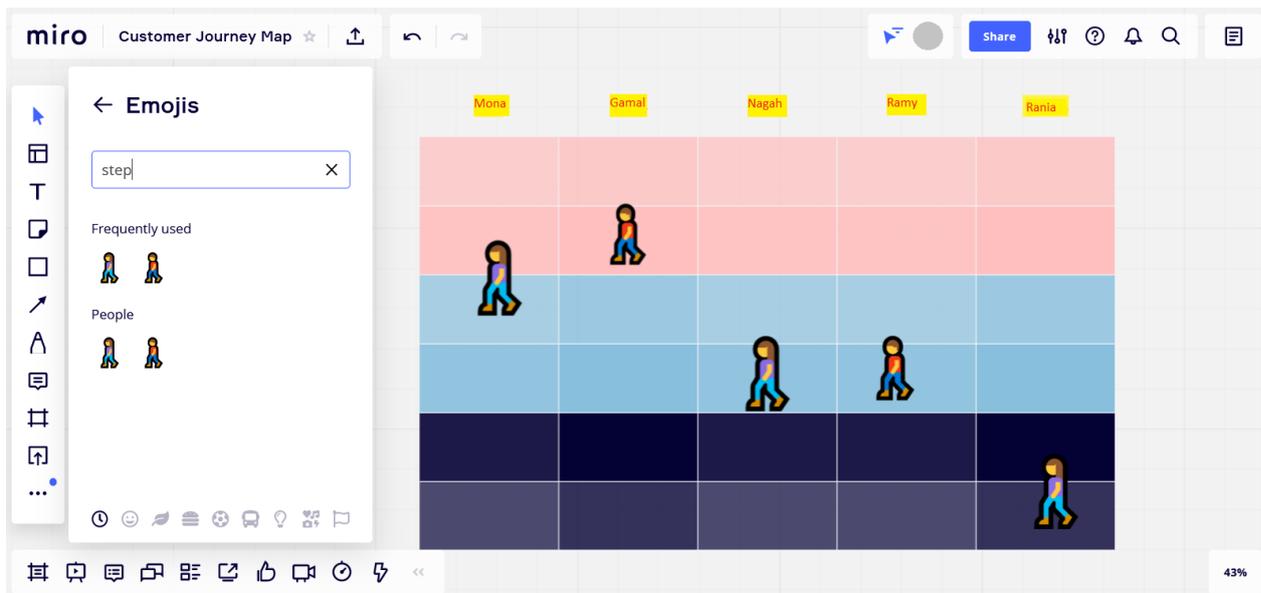
Source- adapted: Online Civic Education Lab.
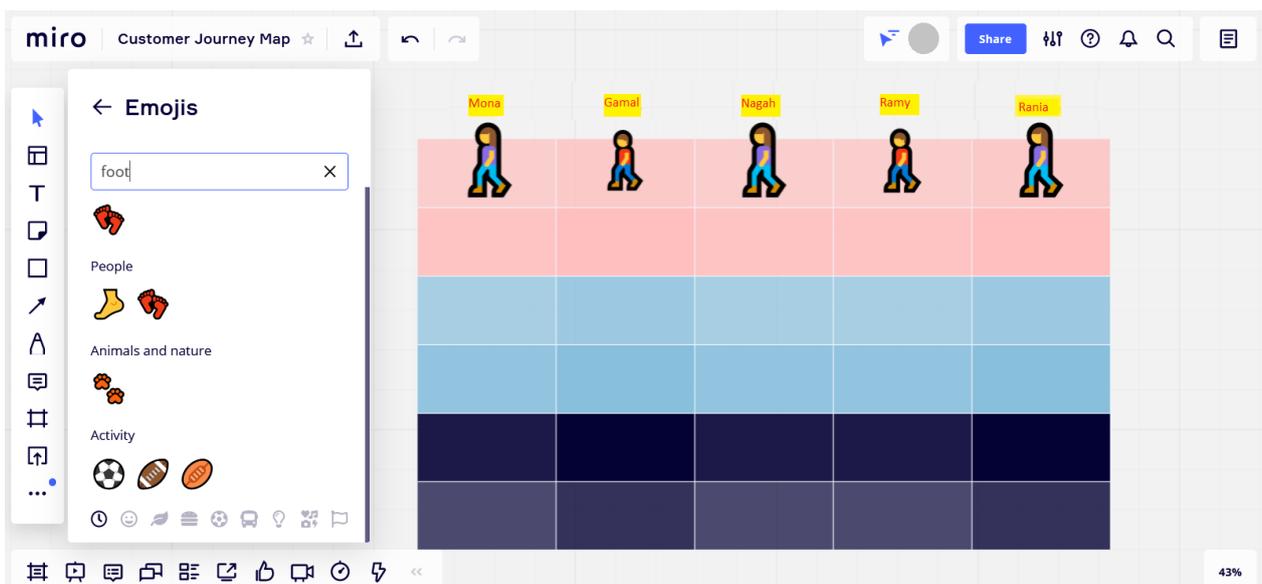
Diversity activities:

Diversity activities are characterized by creativity and innovation of different tools, based on action and the use of the training room and open spaces, such as the "Step Forward (Power Path)" activity. It's hard to imagine doing the same activity online using a meeting program, but it's not impossible using remote training tools.

Step Forward (Power Path):

- Prepare a board on Miro website, containing a table with the expected number of steps x number of participants, adding the names of the participants in front of each column + a symbol for each participant.

- Send messages to participants describing their characters as in role-playing activities, then send the board link to the group, and when making sure that everyone is on Miro without problems, keeping the meeting program unmutes, start reading the phrases one by one.
- Ask the group to move their pieces in the direction of the last row (purple) whenever they agree on any phrase.

- At the end, everyone returns to the room and a discussion is opened about the outcome, roles, and the topic of the activity itself (human rights, freedoms, discrimination...etc.).
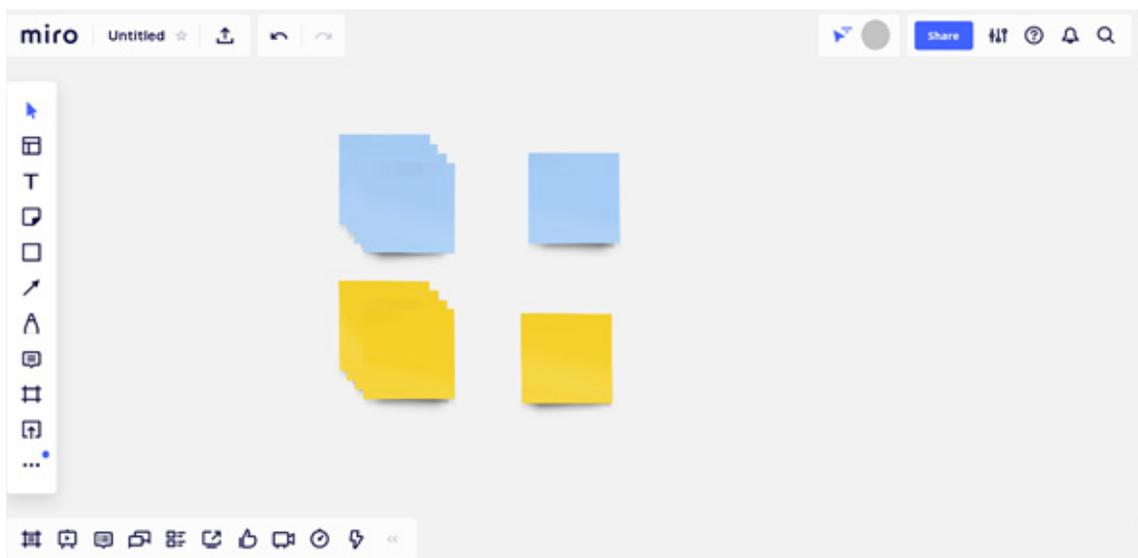
Source- adapted: Activities Report for the Online Civic Education Lab.
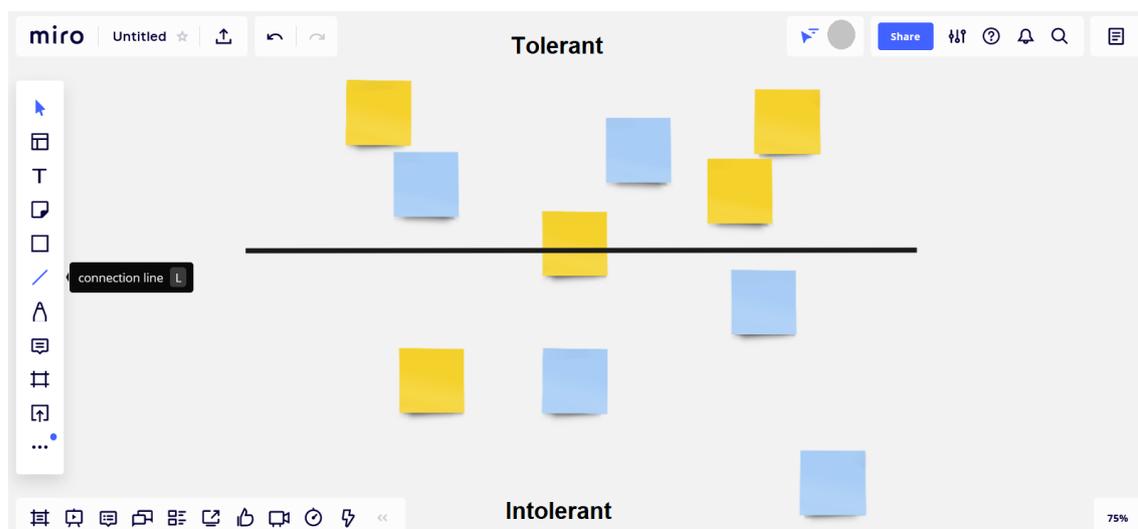Step Forward Activity: The Peacelab Guide.

Obstacles to accepting otherness:

With the same way used in the Step Forward activity, many activities that were originally based on the actual space utilization of the training room can be carried out.

▪ In "Obstacles to accepting the other" activity, the participants are requested to think of societal groups that they do not accept (individually) - for example: corrupt officials.

▪ Then they are asked to think about groups which are totally different from them, but they can accept, for example: another religion followers.

▪ Send them a link to the activity board that enables them to write the different characters/groups with a request not to repeat any of them. (For example, the groups from the first group are written in blue, and the characters from the second group are written in yellow).

▪ After completion of characters, we draw a line expressing the limits of tolerance/acceptance, and all participants must move the characters close to or away from either side of the line; One side should represent "what comes close to their ability to embrace the other" and the second "exceeds their ability to embrace the other."

▪ Getting back to the main room and discuss the results and main objectives of the activity.
Source- adapted: Online Civic Education Lab.
Embracing otherness obstacles activity: Civic Education Manual, page 50.

Group contributions can be gathered as impressions, ideas, suggestions, and evaluation of the workshop in more than one simple way, including:

▪ The Zoom polling tool (prepared on zoom.us before the start of the meeting) to measure the group's overall satisfaction with the various components. This may be followed by an open discussion to hear the different views on the meeting platform.
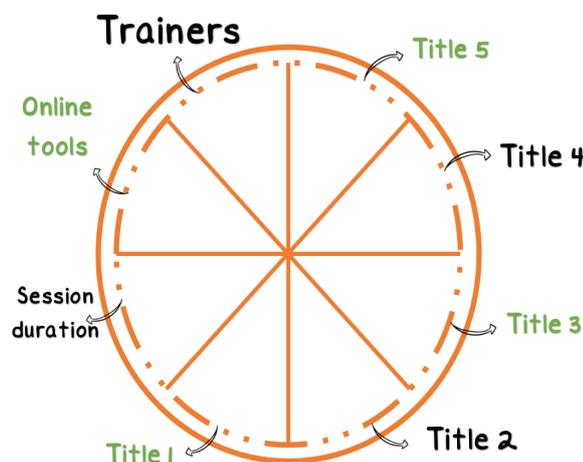Steps of creating a poll on Zoom.
Video demonstration of how to create a poll on Zoom.
▪ A questionnaire on Google forms or any alternative platform, which includes space to answer in detail, multiple choice, scale assessment, and other available features. One of the advantages of this tool is to collect participant data or allow more honest details to be shared anonymously.
▪ Use a collaborative presentation platform such as Google slides and share the link with the group (or split participants into several groups to facilitate discussion and brainstorming among). On the platform, several attractive slides are prepared containing the questions to be answered and the titles to be evaluated, and make sure that there is enough space for the expected number of answers.
▪ Using a whiteboard, a picture can be shared, and participants draw or write to show their impressions, as the following examples:

Evaluation pizza

Group members put a dot in front of each title on the slice of pizza, the closer to the edges = I like, the closer to the center of the circle = I dislike.

Personalities tree:

Participants choose one of the characters by placing a dot or writing the name of the participant next to the figure.

The characters express the general state or current feeling after the workshop or after completing an activity (such as choosing a character that expresses the state of learning and growth, enjoyment, confusion, searching for a meaning...etc.).
After selecting the characters, the participants can be given some time to explain why they chose that character.
- Inspired by Pip Wilson blob tree

Additional tips for remote training:

- **Facebook**

In case of difficulty to use the previously recommended programs and platforms (due to weak connection, or limited capabilities of the used devices...etc.), the simplest tools such as social media platforms can be used.
For example, create a Facebook group and display the content of the sessions in an organized manner according to a schedule, and the participants can interact by writing comments or uploading new posts. Facebook offers the Facebook rooms feature, which enables you to hold a video meeting without the need for an external platform.

Privacy and digital security risks should be taken consideration when using this tool.
- **Use a cloud storage platform** (e.g., Google Drive or Dropbox) for the whole session and share the link with the group. A session file is created and the content, images, and used slides are uploaded to it. This is an alternative to the wall in real training rooms where the facilitation boards are put at the end of each activity.
- **The internet** is filled with content on conducting online sessions, for instance this article has some tips for " Spice up an online wprkshop"
https://www.eventbrite.co.uk/blog/ideas-spice-up-online-workshop-engage-audience-ds00

References:

- «Our Steps Continue « guide, Anna Lindh Foundation (The Egyptian Network), Partners for Transparency, Foundation2020.
https://bit.ly/2RGeIAA

- Dr. Muhammad Hamza, Training Material Preparation Manual, Swedish Civil Emergency Agency, 2014

- Training Management Manual for Civil Society Organizations, USAID, Jordan, 2011
Miscellaneous Topics Muzn Platform for Non-Profit Technology:
https://www.mozn.ws

Training Guide: Safe Chatting Using Jitsi:
https://digital-protection.tech/2018/07/22/jitsi

- Miscellaneous topics on the SURVEILLANCE SELF-DEFENSE platform:
https://ssd.eff.org

Miscellaneous topics on the «Your Safety Wiki» platform concerned with digital security:
https://salamatechwiki.org/

Middle East Newspaper: 6 ways to protect your privacy on Windows 10:
https://bit.ly/2ZMgHUW

-The Civic Education Manual, Goethe-Institut Cairo, Munich - Cairo, 2017:
https://bit.ly/3uPN8ig

- The «Peace Lab» handbook;, Goethe-Institut Cairo, Cairo, 2020:
 https://bit.ly/3fL2dO2

- Reham Refaat, A report on conducting online sessions using the "Online Civic Education Lab" Manual, Goethe-institute Cairo, 2020:
https://bit.ly/3wTaGnY

- Romeral Ortiz, Youth and Peace, Toolkit, United Network of Youth Peacebuilders (UNOY), 2018:
http://bit.ly/38v1KIZ