# CYBERWOMEN


# Introduction

# Introduction




https://iwpr.net/

# Contents

# Introduction to Cyberwomen

Within the last few years, various efforts have been undertaken to create improved resources, methodologies and practices for digital security trainings; however, very few of the resulting outputs have incorporated a strongly developed gender perspective. More recently, thanks to efforts within women's and feminist movements worldwide, a body of gender focused digital security content has begun to emerge – however, there remains a lack of coordination within the digital security community to grow this collection of resources in a strategic, responsive manner.

To that end, the Institute for War and Peace Reporting (IWPR) built the Cyberwomen curriculum with the intention of reflecting the rich technique and practice developed by women human rights defenders (WHRDs) leading digital security training efforts in the Latin America and Caribbean (LAC) region. Based on the experience of working with these women, we have created original training content with the aim of presenting a collaboratively-developed approach for training WHRDs on digital security from a holistic, gender-based perspective.

To avoid duplication of efforts, where we identified existing training materials already responsive to the needs of WHRDs – for example, those found within the LevelUp curriculum, or developed by organizations like Tactical

Technology Collective (TTC) and Association for Progressive Communications (APC) - such content was incorporated directly into the curriculum and cited accordingly. However, the core value-add of this resource lies in originally-produced modules and recommendations designed to offer learning experiences specifically tailored to the context of WHRDs working in high-risk environments.

## Using the Cyberwomen Curriculum

This curriculum was designed with two specific user-profiles in mind: women trainers seeking to deliver gender-focused digital security trainings to women's groups, and members of these women's groups who, after receiving such training, now seek to pass that digital security knowledge onward to their own networks of colleagues and activists. In truth, not all sessions may be relevant to all audiences, and we encourage you to identify which sessions are most valuable for your specific audience and focus exclusively on those.

Cyberwomen includes interactive games, as well as audio-visual and graphic materials, as instructional aids for trainers; furthermore, its modules can be used either as stand-alone sessions or as components of a full training workshop. This modular structure allows trainers to select specific session content to match the needs of training participants; alternatively, trainers may also choose to follow suggested sequences of modules. From start to finish, to cover the entire curriculum would require approximately ten full days; for those trainers who wish to provide such a training, we strongly recommend separating delivery out into a series of workshops spaced over a period of at least six months. This approach will allow participating women the time required to effectively integrate new techniques and tools into their personal digital security practice, before moving on to acquire new skills.

Furthermore, as part of its focus on holistic security, the curriculum incorporates specific content on feminist self-care and recognizing gender-based violence, whether symbolic or online. The objective of these sessions is to reinforce participants' sense of agency and control over their safety and iden-

tities – therefore, it is important that they be integrated throughout trainings as spaces for individual and collective action and reflection, rather than covered as a standalone module by themselves.

Finally, there are many exercises included in this curriculum - some are trust-building exercises, which should be done at the beginning of the first training day; others are basic icebreaker exercises, which can be done at the beginning of any training day. Finally, there are several exercises designed to reinforce specific training content which should only be done in their listed order. The curriculum also includes resources for follow-up sessions to be delivered over the suggested period of six months.

**A Feminist Approach to Curriculum Development**

As mentioned previously, this curriculum integrates a holistic vision of security for WHRDs, including the "Triad" of digital security, physical security and self-care; however, the core of the training is focused on digital security. To integrate a more gender-sensitive, feminist approach, this curriculum was produced with the following core values and principles in mind - we strongly encourage trainers to take these into account while planning workshops using this curriculum:

**Women Participants and Women Trainers**

First and foremost, Cyberwomen content is designed to support an ambiance of woman-to-woman confidence and trust in a training setting. Participants in digital security trainings frequently come from places – both physical and emotional – of high stress or anxiety; women human rights defenders are also frequently the targets of harassment and violence both online and offline. It is paramount that women participants perceive a training as a safe space, where they can feel at ease sharing their fears, doubts and emotions, and can actively participate and engage with others; therefore, this curriculum is intended for women trainers working with women participants. However, we also encourage male trainers to review this curriculum and its foundational

principles to better adapt their own training practice to working with mixed groups in a workshop setting.

**Female and Feminist Models**

This curriculum was created with a focus on sharing real-life instances of digital attacks - as experienced by women human rights defenders, activists and journalists - using empowering testimonies. Recognizing that not every woman at a given workshop will define herself as a feminist, the curriculum's approach to the training process focuses on raising awareness about online violence against WHRDs, first by highlighting differences between attacks on male and female activists, and then by providing examples of online gender-based violence (e.g. on social media platforms) as a means towards helping women identify the violence they may already be facing in these spaces. As part of this methodology, we presented case studies that were close to the women's everyday life, making it easier for participants to relate to different situations and thus understand the relevance to their own context. We found that using this approach empowered participating women to more consistently practice new skills and subsequently provide digital security advice to others.

**My Body, My Devices, My Decision!**

The central ideas, information and practices shared in this curriculum are grounded in promoting digital autonomy. Central to the design of this curriculum is an emphasis on "strategic thinking about digital security" - sharing digital security concepts with participants, rather than just training on a list of tools. A great deal of time is dedicated to introducing participants to digital security concepts such as encryption, anonymity, privacy and open-source software before training on related tools. By empowering women to develop a personalized understanding of these concepts, they come away equipped with the information they need to make their own decisions about which tools are best for them.

**Analysis of Gender-Based Risk and Social Media**

By using examples from YouTube videos, messages on various social media platforms, and outputs emerging from other training sessions, this curriculum aims to hold a safer space for discussion and reflection on technology-based violence that specifically targets women. Specifically, much of this comes together in the Online Violence Against Women module; likewise, the Gender-Based Risk Model exercise found in the module Determining the Best Solution is focused on sharing experiences and identifying vulnerabilities participants face not only as women but as human rights defenders (in this case, in the LAC region).

**Feminist Self-Care & Digital Self-Defense**

As part of a holistic approach to security, this curriculum considers emotional well-being and self-care as a vital element of security for WHRDs; likewise, as part of a focus on digital autonomy, there are specific sessions —the session Gender-Based Risk Model again serving as an example— which are intended to help participants prepare for and react to digital attacks. This curriculum is an effort to provide information for participants to identify and explore several strategies for their digital self-defense; these include, but are not limited to, separating the personal from the public, creating online identities, 'doxxing the troll', encrypting their communications, and documenting digital incidents. By equipping participants with a better understanding of their online environment —across both the platforms they use and the risks associated with each— we can empower them to develop strong digital security habits that can in turn become part of a holistic practice of self-care.

# Planning resources

- **Objective(s):** Pre-training assesment and evaluation

### Pre-Training Assessments

que ondis?

Crucial to the training planning process is gathering the data points needed to design a training agenda. A solid understanding of participants' digital security needs often means the difference between an effective training responsive to participants' goals and context, and an ineffective training potentially exposing participants to greater risk than they were previously.

Knowledge of how potential participants use technology, how they communicate with it, and what prior digital security knowledge they may possess will have a significant impact on the scope of content to be covered.

### Assessing Needs and Motivations

Ideally, you will be able to carry out a needs assessment ahead of your training, by working either with the training participants themselves or with a member of their representing organization. Bear in mind that beyond objectively assessing their needs, it will be important to also understand their motivations for participating in a training – are participants proactively seeking to boost their own resilience, or are they requesting assistance in response to recent or ongoing incidents? Furthermore, from a practical standpoint, knowing how much time you have available ultimately determines how much content you can cover in a single workshop (or subsequent ones); this is furthermore determined by the collective skill level of the participants.

If you have the opportunity for in-depth interaction and communication with participants before your training, below are some questions to ask that can help you learn more about them and/or the organization they work with:

- What is their organization's background?
- How is their organization's team configured?
- What are their organization's main programs and/or activities?
- What are some of their technology-related practices? How and from where from do they access the internet?
- Which type(s) of computers and/or mobile devices do they use? Do they have separate devices for work and personal use?
- Which operating system(s) do they use?
- What other movements or groups do they collaborate with? This can be as a representative of their organization (e.g. as coalition members) or personally as independent activists.
- Have they ever experienced any incidents or direct threats to their physical or digital security? This could be related to their devices, equipment, online accounts or physical aggression.

**Digital Security and Capacity (DISC) Tool**

If there is the opportunity to engage in a comprehensive assessment process with training participants in the time leading up to your workshop, included in this curriculum is the DISC (Digital Security and Capacity) Tool, a resource which IWPR has produced and used extensively for assessment processes ahead of digital security trainings.

The DISC Tool is a pre-training assessment questionnaire that uses a quantifiable scoring mechanism to gauge participants' existing digital security skill level, while also providing qualitative information on strengths and areas for improvement at a more granular, practice-specific level. If you will be working with participants on an iterative basis (for example, leading several trainings over a 6-month period), DISC Tool is also a useful way to track their learning and comprehension progress.

The full DISC Tool resource can be found here[1]

**Alternative Assessment Strategies**

In the event that you're not able to perform a pre-training assessment directly, or have these questions answered, you can still infer quite a bit of background information from what you do know about participants' context and circumstances:

For instance, if you're aware of women activists or organizations conducting similar work in the same region as the group(s) you will be working with, it is likely that any risks or attacks they have faced will be similar in nature to those that your participants might have encountered.

Furthermore, there may be certain known threats or incidents that you can correlate to the kind of work that your participants do (and where they do it). If you will be training women lawyers providing legal counsel to other WHRDs, or women journalists reporting on government corruption, you may be able to research some of the tactics that governments or other non-state

[1] https://cyber-women.com/en/DISC/

actors in their country have used in the past against individuals, in particular women, doing similar work.

## Example training agendas

Although we are aware that the final content of a training session will be based on the diagnosis each trainer does of the group the will work with and we invite each trainer to adjust this session to better meeting the needs of the group, we do suggest a few options for what we think could be regular scenarios of trainings.

The example agendas below are organized by length (in days), and then by participant skill level. Other planning parameters will of course inform the ultimate design of your training; however, time is almost always the most critical:

How much time you have available ultimately determines how much content you can cover in a single workshop; this is furthermore determined by the collective skill level of the participants.

You're more likely to know how many hours or days are available to work with a group before knowing other factors, such as the venue, the number of participants, or their collective skill level.

Read more[2]

Although we are aware that the final content of a training session will be based on the diagnosis each trainer does of the group the will work with and we invite each trainer to adjust this session to better meeting the needs of the group, we do suggest a few options for what we think could be regular scenarios of trainings.

The example agendas below are organized by length (in days), and then by participant skill level. Other planning parameters will of course inform the ultimate design of your training; however, time is almost always the most critical:

[2] https://cyber-women.com/en/agendas/

How much time you have available ultimately determines how much content you can cover in a single workshop; this is furthermore determined by the collective skill level of the participants.

You're more likely to know how many hours or days are available to work with a group before knowing other factors, such as the venue, the number of participants, or their collective skill level.

# Acknowledgments

Some sessions and other information adapted for this curriculum were originally developed by: Association for Progressive Communications, Tactical Technology Collective, Fundación Karisma, Mujeres Al Borde, Elis Monroy from Subversiones Collective, Danah Boyd, Mariel García, Alix Dunn, Spyros Monastiriotis and Phi Requiem.

- **Authors of Original Content and Systematization:** Alma Ugarte Pérez, Indira Cornelio Vidal y Hedme Sierra Castro
- **Coordination:** Dhaniella Falk ,Alejandra Garcia and Dianna James
- **Education and Localization:** Nicholas Sera-Leyva, Azza Sultan, Mohammed Al-Maskati and Ali Sibai
- **Spanish translation:** Nadège Lucas Pérez
- **Coordination of Peer-to-Peer Learning and Session Pilots:** Estrella Soria
- **Consultancy:** Tierra Común cooperative[1]
- **Web development, graphic design and media production:** Kéfir cooperative[2]
- **Peer Reviewers and Collaborators:** Azza Sultan, Carol Waters, Dalia Oth-

[1] https://tierracomun.org
[2] https://kefir.red

man de Tactical Technology Collective, Estrella Soria, Erika Smith from the Association of Progressive Communications, Gigi Alford, Jennifer Schulte, Laura Cunningham, Lindsey Andersen, Megan DeBlois from Internews and Sandra Ordoñez.

# Cyberwomen Data Use Policy

This document was last updated the 4th of September of 2018. Written by Kéfir.

## Context

Before plunging into specific details on how we use the data generated on this site and what you can do to be more agent in all of this, we are going to give some context.

### About the project

The Cyberwomen curricula was created and implemented by the Institute for War and Peace Reporting as part of the project Safety, Awareness and Action (SAWA) and funded through the Bureau of Democracy, Human Rights and Labor (DRL) at the U.S. Department of State.

The web platform was designed and developed by Kéfir[1], as well as the

[1] https://kefir.red/

frontend web and graphic design. Kéfir, until present, administers the server where this project is hosted.

You can read more about the Cyber-Women project here[2].

## The Right to Privacy

The Right to Privacy is defined as a human right, explicitly stated under Article 12 of the 1948 Universal Declaration of Human Rights:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

## Regulations

Apart from human rights, there are specific data regulations. Perhaps you have heard the recent GPDR?

The "General Data Protection Regulation"[3] came into effect the 25th of May of 2018.

This European regulation is designed to better protect citizens from data breaches and privacy violations. The new law is amongst other things stipulating how companies must handle their customers' data.

Unfortunately, these regulations aren't applicable in all contexts and they are not enough standing alone. Certain jurisdictions have a fairly good understanding and coverage of privacy; others are far behind. There are groups and people that, from the policy front-lines, are fighting to change this unequal access to privacy.

[2] https://cyber-women.com/en/#about
[3] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Have a look at the Association for Progressive Communications network's statement on GPDR[4].

## Compliance

All websites and platforms visited by citizens that are protected by data regulations must provide a compulsory legal document that explains how they collect, retain and share personally identifiable information.

Personal Identifiable Information (PII) is any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly. Examples of sensitive PII elements include, but are not limited to: name, social security number, driver's license and other government identification numbers; citizenship, legal status, gender, race/ethnicity; birth date, place of birth; home and personal cell telephone numbers; personal email address, mailing and home address; religious preference; financial information, medical information, disability information; spouse information, marital status, child information, emergency contact information.

Collecting and using data doesn't necessarily have to be a harmful. Data is used for satisfying legal and funding-related reporting requirements and improving tools. What is important is that there is transparency of how data will be collected, stored, processed and shared.

## Cyberwomen's commitment to privacy

Beyond complying certain minimums, this platform, in it's bones and code, was designed and developed by activists to pursue and embed privacy as a value and ethical standpoint and practice.

We don't just avoid identifying individuals but believe in not generating data that can be used for interests that aren't aligned with those of whom visit this platform.

[4] https://www.apc.org/fr/node/34716

Typically, data use policies are abstract, lost in small print and quite cryptic. This reflects a lack of transparency and accountability, normally with the intention of hiding the details of a data business model and collaborations with third parties that users wouldn't be happy to find out about.

In Cyberwomen, our Data Use Policy is an extension of the project: an opportunity to learn about our right to privacy, how it can be taken into account and what specific measures we can apply.

## What we are doing

### Cookies and third party code

When you visit a webpage parts of the page may come from domains and servers other than the one you asked to visit. This is an essential feature of hypertext, but it has also come to be a serious privacy problem. On the modern Web, embedded images and code often use cookies and other methods to track your browsing habits — often to display advertisements. The domains that do this are called "third party trackers"

Internet cookies are, ultimately, text files that a website stores in your computer when you visit so that, in potential future visits, it "remembers" information like your language preference or your log-in.

The CyberWomen platform doesn't use cookies or any type of third party code.

### Communications

Websites that include contact forms must describe why they are asking for such information and what they are going to do with it afterwards. For example, if it going to be used for a newsletter or a database.

Cyberwomen doesn't use contact forms. It does have associated email accounts so people can contact with the project (contacto@cyber-women.com)

and request information related with privacy aspects (privacy@cyberwomen.com).

These mail accounts are also administered by Kéfir that commit to implementing up-to-date security measures, maintaining non-identifiable data logs that are collect only information strictly necessary for it's functioning and that are deleted after one week.

The email accounts are accessed via webmail and email clients, taking into account security practices mentioned in the curricula.

### Logs and web statistics

A log is a record. Services and applications that run on a device tend to save some type of record. This provides information when improving tools and solving possible errors. Generally this information is useful but it contains personal identifiable information like IP addresses and usernames that can be used to create fairly accurate profiles about people's behavior. This is why it is important to anonymize logs in a secure way.

Kéfir's servers don't log any IP addresses, just anonymized visits, which we remove after a week.

Cyberwomen collect statistics, through https://sinapsis.kefir.red, Kéfir's self-hosted version of Piwik/Matomo[5], which means only IWPR and Kéfir have access to this data. It is configured to not log any information that may identify individual visitors, like IP addresses. Also, all individual visits are converted into statistic data and then discarded after a month. Matomo also respects the Do-Not-Track feature browsers specify as a way to opt-out of these kind of systems.

### Javascript

The Cyberwomen site uses javascript.

[5] https://matomo.org/

- zepto.min.js: Zepto[6] is a minimalist JavaScript library for modern browsers with a largely jQuery-compatible API
- agency.js: Cyberwomen is based on Agency Jekyll Theme[7]. This javascript gives the site a responsive menu behavior.

If you disable javascript (using Tor Browser Bundle, through a plugin or through your browser configuration), the site will continue to work. On small screen devices, the menu will appear at the bottom of the page.

### Changes to this Policy

This document may be updated in the future. Come back to this page to see updates.

### Contacts

All questions related to the Data Use Policy can be sent to privacy@cyber-women.com.

## What you can do

You can also contribute to your privacy. The fact that on our side we don't collect data that you don't consent to, that we store it for a limited time in a anonymized way and don't share it with third parties beyond general information for funding report back purposes doesn't mean that other potential intermediaries are vulnerating your privacy.

- Read the Cyberwomen curricula[8] and implement safer practices ;)
- Install the Privacy Badger browser plugin[9]

[6] https://zeptojs.com/
[7] https://github.com/y7kim/agency-jekyll-theme
[8] https://cyber-women.com/en/#modules
[9] https://www.eff.org/privacybadger/

- Configure your Firefox browser to opt out of tracking[10]

## How do I change my cookie settings?

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set, visit https://aboutcookies.org or http://www.allaboutcookies.org/

Find out how to manage cookies on popular browsers:

- Google Chrome[11];
- Microsoft Edge[12];
- Mozilla Firefox[13];
- Microsoft Internet Explorer[14];
- Opera[15];
- Apple Safari[16].

To find information relating to other browsers, visit the browser developer's website. To opt out of being tracked by Google Analytics across all websites, visit https://tools.google.com/dlpage/.

[10] https://support.mozilla.org/en-US/kb/how-do-i-turn-do-not-track-feature

[11] https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=en

[12] https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy

[13] https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

[14] https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies

[15] https://www.opera.com/help/tutorials/security/privacy/

[16] https://support.apple.com/kb/ph21411?locale=en_US