Digital Literacy 101:

WORKSHOP MATERIALS

GNP+
GLOBAL NETWORK OF PEOPLE LIVING WITH HIV

YET4H

Introduction

This is an introductory, youth-friendly digital empowerment training that is a useful resource to improve young people's understanding of, and their ability to advocate for, their rights in the digital space. This digital training and workshop package have been developed in consultation with diverse communities using participatory methods.

The workshop materials in this document aim to support workshop facilitators in increasing the digital literacy of youth communities in three key areas:

1. The harms of digitalization
2. Digital resilience
3. Improving our rights

Potential workshop objectives include:

- Equipping participants with the tools to assert their rights when accessing health data
- Increasing participant skills to verify health data and find accurate sources online
- Providing participants with the tools to protect themselves and their personal information

The overall workshop structure involves three blocks with guiding questions along with a selection of activities designed to help participants explore the guiding questions. Facilitators may select the activities that are most suitable for their target audience, aims, and other contextual factors, but we share two recommended paths in the 'Workshop agenda' below.

The workshop can take place in person or online with remote tools such as conference platforms, virtual white boards and collaborative documents. If working remotely, it's best to have at least one facilitator, someone to serve as tech support for smooth transitions into breakout rooms and collaborative spaces, as well as handling individual connection issues, and someone to take notes if you need to document or reflect after the workshop.

As you read through these materials, look out for the following emojis:

 : goal

 : method

 : tip

We hope you have fun, learn a lot and help young people feel safe and confident as they navigate digital health!

Workshop materials content

This document includes:

Workshop agenda recommendations

SHORTER VERSION

90 minutes

- Introductions *10 mins*
- The journey of my data - *15 mins*
- Balancing risks *15 mins*
- Truth or not? *20 mins*
- Searching the internet *15 mins*
- Closing and additional resources *15 mins*

LONGER VERSION

180 minutes

- Introductions *10 mins*
- Spectrogram *25 mins*
- Data stories *30 mins*
- Balancing risks *15 mins*
- Truth or not? *20 mins*
- Searching the internet *15 mins*
- Well-being in the digital age *20 mins*
- Knowing my rights *30 mins*
- Closing and additional resources *15 mins*

Curriculum

The workshop is designed to be focused on activities, but the guiding questions in each block can be used to prepare the facilitator, introduce and support activities, and/or encourage reflection and discussion. The links and information that follow each guiding question can be shared as necessary and when relevant. For instance, if participants are having trouble thinking about how data can be misused, you might share some of the examples listed in Block 1.

BLOCK 1: The harms of digitalization

- What data is out there about us? Who holds that information? Who else may access?
- What happens if our data gets into the wrong hands?
  - Nobody's Business But Mine, Privacy International's work on menstruation apps and data exploitation
  - 2018 story on Grindr sharing HIV status with third-party vendors, Vox
  - How Digital Health Apps Can Exploit User Data, Privacy International
  - Suicide Hotline Shares Data with For-Profit Spinoff, Raising Ethical Questions, Politico
- What stories can be told about us with that data? How can those stories harm us?

Activity: Data stories (30 minutes)

To understand the assumptions that can be made about us with only a few data points.

Open discussion, moving to individual reflection and small group work, and back to main group discussion.

If people are quiet in open discussion, pick an app you know many of them use and ask the group, "What might someone learn about you based on your use of this app?" Encourage people to type, raise their hands, unmute and/or type in the chat.

Open discussion: The apps we use collect data about us. In small groups, look at the apps our imaginary person, Chandra, uses frequently. Consider the kind of data each app might be collecting and what that data might tell us about Chandra. What happens when you put all of these datasets together?

Chandra's most-used apps include:

- Google Maps for directions to appointments and events
- Uber Eats and Zwiggy for food delivery
- Remitly for sending money to friends
- TikTok for laughs
- Zoom for meeting with their therapist
- Spotify for music and podcasts
- Google Search for looking up everything

Individual reflection and small group (2-3 people) work: Now take a few minutes to make a list of your most-used apps and some of the data you think these apps are collecting. Talk with your small group mates about what kind of story, true or not, can be told about each other.

Report back to main discussion: How did this make you feel?

Activity: The journey of my data (15 minutes)

To explore the data we are sharing and what may be happening with it.

Individual reflection preferably in one shared document or platform like EasyRetro.

Play some lofi music while participants are working to set a thoughtful, creative tone instead of sitting in silence.

Answer the questions in the table for yourself (copy/paste the table into your own doc, write it down in a notebook, etc.) to the best of your knowledge.
See the example in the first row to help you get started. Afterwards, feel free to share with the group something you learned or wondered about. On your own time, you can use this table to find more answers in terms of service or consent forms. You can also use it as a way to evaluate apps and other tools you are interested in before you download or register, allowing you to make more informed choices..

Who has my data?	**How did they get it?**	**Is any of that data sensitive?**	**Is it necessary for the service they provide?**	**How are they using my data?**	**Who are they sharing my data with?**	**What would happen if it got into the wrong hands?**	**Is there anything I can do about it?**
Health chat forum	*From account details, maybe from what I've said in the forum?*	*Yes! My sexuality and HIV status*	*No, only some account info like email*	*I don't know*	*No one, I hope. But I don't know*	*I might lose my job or be kicked out of my church*	*Check the terms of service and look for a more secure forum if need be*

- How does mis-and disinformation spread online?
  - Gendered Disinformation on Monkeypox, Association for Progressive Communications
  - Content tactics and mistakes to watch for: Bait headlines, opinions stated as fact (often opinion pieces are presented on social media as fact), lack of sources, partisan or untrustworthy sources posing as fair or legitimate, lack of context, single data points (the single data point in the bait headline gives the wrong impression), photoshopping, deep fakes
  - Digital tactics to watch out for: Bots, sock puppets, targeted ads, paid influencers, flooding spaces, suppressing information

BLOCK 2: Digital resilience

- Where can we find existing laws and regulations that can help assert our rights in digital spaces? Which organizations and activist communities provide legal aid or strategic litigation in these areas?
  - https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
  - Global orgs: Access Now, EFF, Amnesty International, Article 19
- What are the other tools and tips we currently have to better protect ourselves online?

Activity: Balancing risks (15 minutes)

To know how to make more informed decisions about the risks and opportunities of digital health.

Individual reflection preferably in a shared document or small group followed by open discussion. If doing small groups, each group should work on one statement.

It doesn't matter if participants are already doing or planning to do what's in the statements. They can work on any one, as the point is to think strategically about what we do online.

Every day we make decisions about taking risks — from crossing the street to eating dodgy leftover food. Maybe you have a big exam in school tomorrow. You need to stay up late and study, but you know that lack of sleep will affect how well you do on the exam, so you decide which option will work best for you or find a compromise between the two. We've talked a lot about risks with data and privacy and surveillance, but we need to be able to use the digital tools we have at our disposal.

Let's figure out how to balance some of these risks with our needs and desires online. Pick one of the following statements and answer the questions below it. Afterwards, feel free to share with the group how you felt about the risks and what you might do.

1. I want to use a chat app where I can discuss health issues with others facing the same issues.
   a. Do you want to share information in your discussions that you don't want people outside of the app to know about?
   b. What would happen if those people found out?
   c. Do you have to use your real name and other personally identifiable information to register?
   d. Does your chosen app have privacy and data sharing policies you feel comfortable with?
   e. Is there any data sharing you can opt out of?
   f. Does the app have end-to-end encryption that makes communication more secure?
   g. If you answered no to questions C-E, is there another chat app that does better on privacy and would you be willing to use it?
   h. If you answered no to question F, are you willing to take the risk in question B?
   i. Are there other steps you can take to protect yourself and your data while using this app?

2. I want to get telehealth by meeting with a doctor remotely.
   a. What would happen if your medical information was shared with a third party you did not consent to (e.g., your family, work, private company, government, the general public)?

b. Does your telehealth provider have privacy and data sharing policies you feel comfortable with?
c. Is there information the provider wants from you (through registration or other forms, for example) that seems irrelevant (e.g., your religion)?
d. Is there any data sharing you can opt out of?
e. Do you know what happens to your data once you are no longer a patient?
f. If the provider uses a video platform, can you access the platform's privacy policies or find information about its security protocols, such as use of end-to-end encryption, or vulnerabilities?
g. If you answered no to questions B, D, E and F, is there another telehealth provider that does better on privacy and would you be willing to switch?
h. If you answered no to question G, are you willing to take the risk in question A?
i. Are there other steps you can take to protect yourself and your data while using this telehealth provider?

3. I want to be loud about HIV-related advocacy on my social media apps.
a. Does your country have strong freedom of expression laws and practices?
b. If not, what might happen if the government sees your advocacy or someone reports it to them?
c. Are you worried about online abuse and how it can cross over into physical violence?
d. If there are people in your life you do not want to see your advocacy, what would happen if they did?
e. Do you have to use your real name and other personally identifiable information to register?
f. Given your answers to A, B, C and D, is there any personally identifiable information you should limit on social media (e.g., full name, city, photos, connections to local people, presence at events)?
g. Do you have a support system of friends and family and/or legal and psychosocial services that can help you deal with punitive responses from the state, online abuse or other serious issues?
h. Does your chosen social media have privacy and data sharing policies you feel comfortable with?
i. Is there any data sharing you can opt out of?
j. Given your answers to the above questions, do you feel it's worth it to take the risk?
k. Are there other steps you can take to protect yourself and your data while using these platforms?

- Refuse cookies
- Use search engines that don't track you (e.g., DuckDuckGo)
- Create strong passwords and use a password manager
- Use end-to-end encryption whenever possible
- Software updates
- Smart phone data
- Read data sharing policies in terms of service carefully, use TOS; dr for simplified overviews
- Check the app privacy section for each app in Apple's app store and Google Play
- Don't connect apps to social media accounts; create separate logins
- Adjust privacy settings on apps and devices to limit tracking, especially social media
- Dating app privacy

- What are the best and easiest methods to find or verify online information?

Activity: Truth or not? (20 minutes)

To identify how fake stories spread online and equip participants with the tools to spot mis and disinformation.

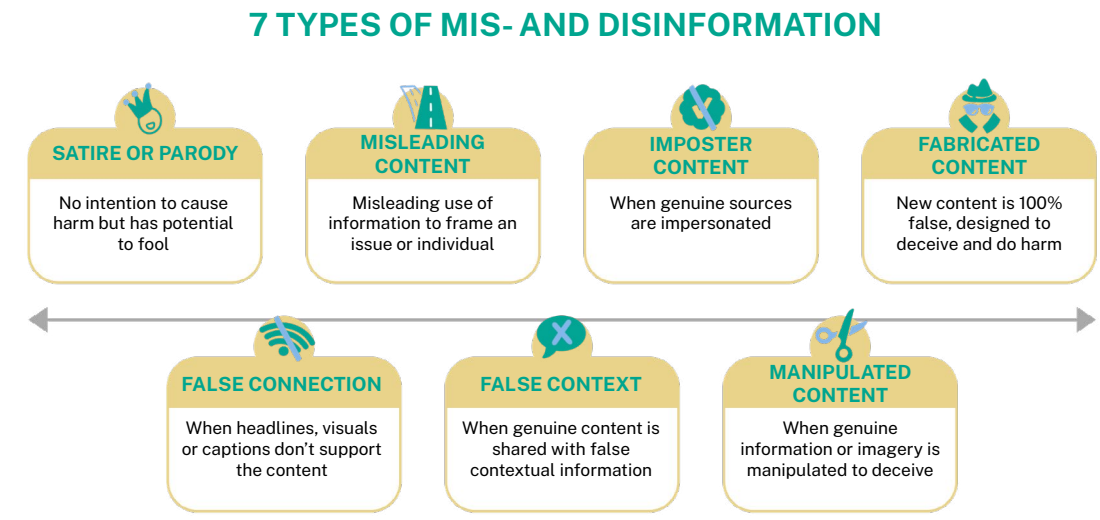
Small groups followed by main discussion.

Before going into breakout groups, share the 7 types of mis-and disinformation graphic below by sharing your screen or copy/pasting into a shared document. Back in the main group at the end, consider sharing fact-checking tactics like SURE, IMVAIN from the curriculum in a brainstorm about how to fact check health-related information online.

We live in an information ecosystem where both facts and inaccuracies can go viral at a very fast speed. Everybody comes across fake stories and inaccurate information online on a regular basis, and we often amplify these stories because we don't know how to check their accuracy.

Let's think about some of the ways and reasons why fake information gets created and shared online, and what we can all do to distinguish between facts and misinformation in our everyday digital interactions.

Each group has seven minutes to come up with health-related headlines for each type — either inspired by stories they came across in the real world or made up by the group. Then come back to the main group to share your favorite headlines, along with why and how you think such headlines go viral.



Source: https://firstdraftnews.org/articles/fake-news-complicated/

- Learn to identify tactics
  - Bot or not?, Tactical Tech
  - Is What You See Really What You Get? Explore Visual Misinformation, Tactical Tech
  - Health vs. Hoax, Tactical Tech
  - Fight Fake News, UNESCO
  - 7 Verification Tools for Better Fact-checking, Reuters
  - IMVAIN method, Digital Resource Center
  - SURE method, Singapore government

- Seek out trusted resources, looking at outlet, author, date, even who financed a study
- Try 2-3 different search engines to see what each brings up
- Explore Google's search tips for inputting keywords
- Cross check information with other outlets or fact-checking sites
- Dig for more details or context

- How to effectively search on the internet?

Activity: Searching the internet (15 minutes)

To practice how to find accurate data online, and how participants can search the internet in smart and effective ways.

Small groups followed by main discussion.

If a speaking participant experiences connection problems in the main group that can't be sorted out quickly, mute them if needed and say and type in the chat that there are audio problems and they are welcome to type their thoughts in the chat or work with tech support to improve audio. This way individual tech problems won't derail the conversation.

Now pick one of your favorite fake stories from the previous Truth or Lie session, and try to find accurate information about the same story, in collaboration with the others from your small group. You'll come back and share what you've found with the main group.

Some of the things to watch out for when assessing a website during your online search:

Authority	Who is the author of the site? Are their credentials stated? Are they considered an authority in that area? (It may be worth checking other resources to find this out) Do they give contact details? What is their purpose in creating the site?
Reliability	Check the domain in the URL. Is it from an educational institution (edu or ac), a government agency (gov or govt), or a commercial organisation (com or co)? What is the purpose of the site?
Currency	When was the site last updated? Is this stated?
Relevancy	Does the information provided by the site meet your research needs? Simply because it is on the internet does not mean it is the best source of information. Check with a librarian for other sources of information.
Comprehensiveness	Is the information on the site thorough? Does it provide information from a number of perspectives or only one?
Accuracy	Is the information on the site accurate? Check against other sources of information if you are not sure.
Usability	How user friendly is the site? Is it quick to load and easy to find your way around? Does it have a search option that allows you to find the information you require?

- Finding good information on the internet, Scientific American
- Finding Reliable Information Online, Leslie Stebbins

BLOCK 3: Digital resilience and data justice advocacy

- What can we do if digitalization is harming our well-being?

Activity: Taking care of our wellbeing (20 minutes)

To identify ways to lessen the stress and anxiety of digital practices.

Individual reflection preferably in a shared document or small group followed by open discussion. If doing small groups, each group should work on one statement.

Participant may bring up heavy topics and experiences. If you're struggling with how to navigate the conversation, focus on listening, affirming, and emphasizing ways to cope. At the end of this document, you'll find resources to share and, if appropriate, consider following up privately with anyone you're concerned about.

I know you might be feeling some stress right now as you think about problems like data misuse and misinformation. We've all likely faced problems related to our use of the internet, like bullying or harassment on social media, doomscrolling, and social comparison. Let's break up into small groups to talk through how the internet affects our wellbeing and how we can take care of ourselves. Pick a note-taker, so you can share highlights when we come back to the main group.

- What are some of the ways the digital world negatively affects our wellbeing? Think about online activities that may have a negative impact on us, like online gambling or social comparison and FOMO, or the ways social dynamics and biases can be intensified online.
- How can we take care of ourselves when this happens? What are some small, practical changes we can make, like turning off notifications or avoiding doomscrolling? What are bigger steps that might be helpful?
- How would we like to feel when online?
- Are there tools, practices, communities we can rely on to help us feel that way online?

- What are the current local and global advocacy gaps when it comes to health in digital rights? How might we identify them? Who are the stakeholders to involve in local advocacy campaigns?

Activity: Knowing my rights (30 minutes)

To understand the ways digital rights and justice apply to health, possible avenues for demanding change, and the support we can seek when those rights are infringed.

White board or sticky notes, main group, small groups and back to main group.

I advance, prepare a space in the shared notes document for each small group to work on their digital health issue with the attached questions.

Whiteboard or sticky notes: In a 2016 addition to the Universal Declaration of Human Rights, the United Nations said, "the same rights that people have offline must also be protected online." On the white board (or on sticky notes), add anything you see that is : 1) a "right" or law in your country, or what you think should be a right or a law and 2) related to our lives on the internet. Think about what people or institutions should or shouldn't be allowed to do, and what they must do. For example,

if my doctor has to protect my medical records at their office, then they have to protect them online too.

Main group: Now that we've thought about rights, let's talk about justice. Sometimes the ways data is collected, shared and used can be particularly harmful for communities like us. How do you want people in digital health to approach your data? How could they help us get the most out of our data for our health? What should they know about how their use of our data might harm us? How can communities like ours take control of our data? Could we be the ones deciding what happens with it? What can we do for digital justice?

Small groups: Now talk through a digital health issue with your small groups and take notes in our shared notes doc so we can learn from each other. The small group questions will help us explore how to advocate for change.

- Identify a digital health issue you want to see addressed in your context. (Examples if needed: excessive data collection and sharing/selling, lack of secure spaces for safe discussion, criminalization or restriction of certain online expression, mis/disinformation around monkeypox, lack of accurate public health data, lack of access to your own health data, internet shutdowns and other access issues.)
- What groups are most affected by this issue?
- Who has the power to take action on this issue? Think about decision makers at different levels (government, private sector, communities, individuals, people just like you, etc.)
- What is the specific action you want them to take?
- What are the best ways to convince or put pressure on them?
- Which groups (grassroot activists, advocacy groups, private sector stakeholders, academia, legal professionals, voters, etc.) can provide necessary support around these issues?
- What resources would you need to get them to take action? What is already available to you? How can you get the rest?

- What reliable and up-to-date toolkits, guidance and resources are out there that we can build upon?
  - Data Protection Guide, Privacy International
  - FOI Guide, Privacy International
  - Strengthening intersectional approaches to data and digital rights advocacy during the pandemic, The Engine Room
  - Policy Explainers, Association for Progressive Communications
  - Internet Governance Forum Dynamic Coalition on Digital Health
  - ICTs for Feminist Movement Building Toolkit, JASS

Closing

(15 minutes)

- To close the workshop in a meaningful, concise and actionable way.
- Individual reflection, followed by main group.
- During this time, the facilitator can share some final resources from the curriculum or ‘Additional resources’ section. One way to do this is to already list them in a shared notes document or other collaborative document and ask participants to add any of their own.

  Take a few minutes to respond to the following questions either in the shared notes doc or wherever you are taking notes for yourself.

  - *What were three key points or ‘take-aways’ from today’s workshop?*
  - *What is a question you have about what we discussed today?*
  - *What do you want to learn more about?*

  Are there any final thoughts or resources you would like to share?

Annex

PRE- POST-SURVEY

Note to facilitators: If you wish, to measure the impact of the workshop, ask participants to take this survey during the time set aside for introductions or prior to starting the workshop. During the closing or after the workshop, ask participants to take it again to see how their responses show an increase in knowledge. We recommend using a survey platform with one link for the pre-test and another link for the post-test in order to tabulate results separately.

Instructions: Please select how much you agree with the following statements on a scale of 1 to 5, with 1 being 'very much agree' and 5 being 'do not agree at all.'

1. I know what kind of data digital apps, platforms and services are collecting on me.
2. I know how to limit how my data is tracked, stored and shared when possible.
3. I am aware of the ways people can be harmed by digital systems and mass data collection.
4. I know how to protect myself online and what tools I have to improve my digital security.
5. I can usually tell if a piece of information I see online is trustworthy or not.
6. I know where to find accurate information online and how to search for the things I'm interested in.
7. I manage my digital boundaries well and have a healthy balance between my online and offline existence.
8. I know my rights when it comes to accessing, using, creating or sharing online content.
9. I know who to turn to for legal protections if my digital rights have been infringed.
10. I am familiar with the toolkits, guidance and resources that can help me navigate the internet in a safe and secure way.

ICEBREAKERS

Introductions: Setting a fun tone (10 minutes)

- To create space for every participant to quickly introduce themselves to the group

  Everybody writes down their name, the community/ies they represent, and one entirely random fact about themselves that they feel comfortable sharing with the group. Everyone reads out aloud and the others can ask questions about the random facts.

Introductions: Setting a fun tone (10 minutes)

- To create space for the group to get to know each other even better, to get a little personal and build trust amongst participants.

  Facilitator draws a horizontal line on a white board app, writing one of the two extremes of the spectrum at each end:

  - *I feel excited and confident about using digital health apps.*
  - *I feel nervous and uncertain about using digital health apps.*

  Ask participants to draw an X somewhere on the line to show where they fall on the spectrum. Ask if anyone wants to share why they feel the way they do.

GLOSSARY OF KEY TERMS

We recommend that facilitators familiarize themselves with the terms below and use these definitions and examples as necessary during the workshop.

- Data point: A single piece of information
  - *Example: age*
- Dataset: A collection of data points, often in relation to other data points
  - *Example: A patient's lab results over the past year*
- Personally identifiable information (PII): Data that could be used to identify an individual
  - *Example: A patient's lab results over the past year*
- Sensitive personal data: Data a person may want to be extra secure and confidential
  - *Example: Data related to a person's sex life*
- Metadata: Data that gives you information about other data
  - *Example: Time stamp on a photo*
- Informed consent: When a person voluntarily agrees to the collection, storage, sharing or processing of their data by another entity. Ideally, consent should be:
    - Freely given
    - Reversible
    - Informed
    - Enthusiastic
    - Specific
  - *Example: A digital health provider walks you through their data process, informing you that they will collect data about your health condition in order to provide appropriate care. The data may be shared with other health professionals on their team in case of complex cases, and any data they use for internal research will be de-identified. Your data will not be shared with other entities. You have the right to change your mind and request removal of your data at any time. There is an opportunity for you to ask questions or seek more information. You feel comfortable with the process and sign the document.*
- Data sharing: Providing partners with access to data they do not already possess. In many cases, this is done with the individual's consent, but sometimes consent is not requested even though it should be.
  - *Consensual example: A healthcare provider shares patient data with the patient's health insurance company according to the terms described in the consent form the patient signed*
  - *Non-consensual example: A healthcare provider shares patient data with a marketing company not mentioned in the consent form*
- De-identification: The removal of PII from a dataset.
  - *Example: A government health agency removes PII such as name, address, and birthdate from datasets on Covid cases before making the data publicly available*
- Mosaic effect: When several data points that would not identify a person when used individually are combined and result in the ability to identify that person.
  - *Example: "Sparked by a study that found Mohammed to be the most common name among New York City taxi drivers, a single private citizen compared Islamic prayer times with publicly available data from the NYC Taxi & Limousine Commission to identify drivers who could be Muslim. Simply mosaicking these two datasets revealed individuals whose periods of inactivity overlapped conspicuously with the five daily calls to prayer. Though the dataset had been carefully stripped of personally identifiable information — names, license plate numbers, medallion numbers — specific, potentially sensitive, groups still came into focus with minimal manipulation."*

- Algorithm: A process that uses data to solve a problem or achieve a task, often by a computer.
  - *Netflix's algorithm uses your viewing history, ratings, data from other users with similar interests, movie data (genres, actors, etc.), the time of day you watch, the length of time you watch and the devices you use to make movie recommendations.*

- Disinformation: False or misleading information shared with the intent to deceive.
  - *Example: A TV news show intentionally takes data from a health study out of context, ignoring the limits of the study and the researchers' analysis in order to promote a politically motivated stance.*

- Misinformation: False or misleading information shared without the intent to deceive
  - *Example: Your family member sees a social media post not knowing that it takes the results of a health study out of context, leading people to believe that a particular precaution is not effective.*

- Bot: An app programmed to do certain tasks.
  - *Example: On social media, bots are usually fake accounts that post, share and like content.*

- Sock puppet: A fake account created by a person.
  - *Example: On social media, one individual will usually create multiple fake accounts in order to manipulate public opinion.*

- Deep fake: Video, audio or image that has been digitally altered to make it look like someone is doing or saying something they did not.
  - *Example: A 2022 video of Ukrainian President Volodymyr Zelenskyy telling his soldiers to surrender.*

- Data protection: Policies, protocols and regulations to safeguard data from loss, corruption and misuse
  - *Examples: The European Union's General Data Protection Regulation (EU GDPR), The Protection of Personal Information Act (POPIA), Covid-19 Data Protection and Privacy Resources, OECD Principles on AI, WHO's Protection of Personal Data in Health Information Systems*

- Digital security: Tools and tips to protect digital devices, accounts and data
  - *Example: Using a unique password/passphrase for each account*

- Digital resilience: The knowledge, skills and confidence to take care of ourselves in the digital age. This can include digital security, tech savvy, digital wellness, supportive networks and resources. It allows us to make the most of our online lives while limiting harm.

- End-to-end encryption: A secure method that prevents anyone but the sender and intended recipient from accessing a message.
  - *Whatsapp uses end-to-end encryption so that not even the company itself can read your messages.*

- Digital rights: A series of rights related to or affected by digital technology.
  - *Examples: Access to the internet, access to information, freedom of expression, freedom from violence, privacy (especially regarding communication and data)*

- Data justice: A just approach to how people are represented by data, especially historically marginalized communities
  - *Example: Transparency in how an algorithm works, including the types of data collected and how they are used to create a recommendation*
- Internet governance: Laws, policies and practices that shape the internet
  - *Example: Dynamic Coalition on Public Access in Libraries*

ADDITIONAL RESOURCES

Data mining

- AdTech, Privacy International
- Micro-targeting, Privacy International
- Data Rights for Communities, Digital Empowerment Foundation
- 'Data is a Fingerprint': Why You Aren't as Anonymous as You Think Online, Guardian

Digital security and self-help

- Escape the defaults, Tactical Tech
- Refresh and Renew: Curate Your Online Identity and Accounts, Tactical Tech
- Digital First Aid Kit
- Self-care, Digital First Aid
- A DIY Guide to Feminist Cybersecurity, Hackblossom
- Take Back the Tech!
- Access Now's Digital Security Helpline
- HeartMob community for people experiencing online harassment
- Online Gambling, Gaming Addiction: Tips That Can Help, Healthline
- How to Overcome FOMO, Psychology Today
- Digital Detox, American Academy of Ophthalmology

Digital health and privacy

- Digital Health: What Does It Mean for Your Rights and Freedoms, Privacy International
- Zoom Privacy Risks, CNET
- Mozilla's examination of BetterHelp's privacy policies

Advocacy and movement building

- Policy Reform: Working Toward Feminist Transformation and Change, GenderIT
- African School of Internet Governance (AFRISIG)
- RightsCon
- MozFest
- Internet Freedom Festival

Acknowledgements

This document was developed by The Engine Room with support from the Global Network of People Living with HIV (GNP+), STOPAIDS and Young Experts: Tech for Health (YET4H).

For questions related to this document, please contact info@yet4h.org