HRDAP
Digital Security Recommendations

HRDAP will be hosted through the HRDAP Platform, a tailor-made learning platform on the ISHR Academy, where you will access:

- reading materials (including on digital security), e-learning courses, quizzes, and more
- the HRDAP Community Space (hosted through Mattermost), where you can discuss topics with other defenders, take part in peer-peer learning, and receive group and individual coaching through instant messaging and video-conference calls (these calls will be hosted through Jitsi)
- Access all live sessions, including peer-peer check-in sessions & Q&As with human rights experts (hosted through Zoom)

We will also use the secure instant messaging service Signal for reminders and chats. This can also be used as a secure alternative to Mattermost on theHRDAP platform to exchange questions with your individual coach should you be communicating sensitive information.

You will soon receive an email invitation from ISHR inviting you to create your account on the HRDAP Platform. You will also receive further instructions on how to navigate the platform. **In the meantime, we invite you to respond to a short risk-assessment and to review our tips and recommendations on how to use these online platforms while ensuring your safety and that of other HRDAPers.**

HRDAP Risk-self assessment: Am I at heightened risk?

To determine how strictly you need to approach digital security, we need to assess the level of risk of reprisals or surveillance you face. By answering the following questions, we will be able to tailor recommendations to better protect your identity and sensitive information in HRDAP digital communication.

- *Do you consider yourself at physical risk (threats to physical integrity) due to your activity as a human rights defender in general?*
- *Do you consider yourself at physical risk (threats to physical integrity) for cooperating with ISHR and/or participating in an international advocacy programme such as HRDAP (including accessing live sessions and online materials)?*
- *Do you consider yourself at risk of intimidation or reprisal due to your cooperation with the UN (whether from sending information or attending a UN session)? This intimidation can come from your Government, as well as non-State actors.*
- *Do you consider yourself at digital risk due to your activity as a human rights defender, that is, exposed to threats of your personal or work-related information being accessed or digital communications surveilled, or other types of digital risks?*
- *Are you working in or on highly restrictive human rights environments and environments under surveillance (including China, Russia, Egypt, Saudi Arabia, Syria)?*

The information below is for every HRDAP participant to consider, but if your answer is yes to any of the above questions, please take the additional extra precautions for "HRDAPers at heightened risk "listed under each section below to keep you and your information secure. Please contact your HRDAP manager if you need help with a specific need regarding your situation for a tailored recommendation.

Sensitive information This includes:

• Information that can identify you or any other HRDAPer at heightened risk or their work;

➔ Guiding question in determining sensitivity: is it problematic if this information falls into the wrong hands?

ONLINE LEARNING PLATFORM: HRDAP Platform & Mattermost

Once you receive an email invitation from ISHR, you will need to create an account on the HRDAP Platform, in order to access all the different materials & the online tools we will be using for the distance learning course. You will also automatically be registered into the HRDAP Community Space (hosted through Mattermost). *Please note that you don't need to create a separate account or go directly to the Mattermost site, as this space will be accessible to you directly through the HRDAP Platform.*

Here are a few tips and recommendations for you all to consider:

- Security Recommendations for HRDAPers, when creating an account for the HRDAP Platform:

  - Use **a secure, unique password for the platform - ideal passwords are passphrases of four unrelated words separated by spaces, with a number and symbol. Securely store these passphrase, ideally in a password manager (More information), and do not store your passwords in your web browser.**
  - **Use 2-factor authentication if possible.**
  - **Be aware of phishing attacks.**
  - Do not share content from HRDAP publicly.
  - Keep everything (operative systems, apps, etc.) up-to-date, with the latest security patches, including an updated anti-virus
  - Be mindful of what information you share, to ensure that you don't put yourself, other HRDAPers, or their work at risk. Also seek the person's explicit content before disclosing any information regarding their identity or work (photo, video social media post, etc). If you have concerns or questions, contact Hannah.
  - We strongly encourage the use of VPN whenever possible.

Additional recommendations for HRDAPers at heightened risk:

- Create a 'fake' email account just for the purpose of registering (**please inform Hannah through Signal that this email belongs to you. You will not be able to enter the HRDAP Platform until Hannah verifies you)**
- Send sensitive information (such as the specific advocacy cases you are working on or sensitive information related to your person or another HRDAPer) via Protonmail (email), Signal (messaging app) or an equivalent encrypted communications channel.
- Disable email notifications.

VIDEO CONFERENCING TOOL: Zoom

All live webinars which will take place with the **entire cohort** of HRDAPers will be hosted through Zoom. This includes the Welcome Webinar & the Wrap-up Webinar, Peer-peer check-in sessions & Q&As with human rights experts and the Discussion meetings with external speakers.

All you will need to enter a meeting is the link & password. You won't need to create an account or register when signing in.

You will receive links to these Zoom calls directly through the HRDAP Platform.

Please note that these sessions will be recorded and shared on the HRDAP Platform exclusively (they will not, and should not, be shared beyond the cohort).

For HRDAPers at heightened risks you may want to keep your webcam off, use a pseudonym when joining the meeting, and avoid giving sensitive information. We will enhance the security features when using Zoom by sharing the password on Signal, and lock the room when the meeting has started. Please always turn on your VPN and connect to a server inside the European Union before joining the Zoom meeting.

VIDEO CONFERENCING TOOL: Jitsi

For video conference calls with your **individual coach & with your group during the group coaching sessions,** calls will be on Jitsi.

Jitsi offers higher levels of security, as it uses hop-by-hop encryption to protect video conference calls, meaning that the video call to the server carries encryption. The server decrypts the video call, then re-encrypts it and forwards it to the video participants.

All you will need to enter a meeting is the link & password. You won't need to create an account or register when signing in.

Jitsi Meet is a browser-based encrypted video conferencing program. You can schedule a Jitsi call in one of the Jitsi trusted server3 listed below:

- *https://meet.mayfirst.org*
-*https://meet.greenhost.net*

To do so, click on one of the links below, then click on 'Go' to start a new meeting, copy the link, and share it through a secure channel with other participants.

You will receive links to Jitsi calls during HRDAP directly through the HRDAP Platform.
When joining sessions, please make sure you:

- Join calls from a quiet space with a webcam, headphones, and a good microphone.
- Make sure you have your phone with you – you may need to log in through the Jitsi app on your phone as sometimes the connection is better than on a computer.
- Close any applications you might not need on your computer – this will slow down the connection.
- Use Google Chrome as your web browser as this works best with Jitsi. Please avoid saving passwords in your browser memory.

Security Recommendations for HRDAPers:

- If you are the one initiating the call and are the host, connect first, create a password (by clicking on the 'i' symbol at the bottom right), and share it through a secure channel;
- Make sure there are no other unknown participants joining the call (if there are, you can expel them by selections the options in their video box);
- Make sure all participants are comfortable turning on cameras (otherwise turn them off);

Additional recommendations for HRDAPers with higher security risks:

- You should use VPN whenever possible while dialling in.
- Consider using a Pseudonym and keep your camera off.
- Keep your personal digital security practices.

INSTANT MESSAGING TOOL: Signal

We will also use the encrypted instant messaging service Signal for reminders, chats and more. This can also be used as a secure alternative to the HRDAP platform to exchange questions with your individual coach should you be communicating sensitive information.

Time sensitive messages: You can send disappearing messages so they will disappear after a set time, by:

- taping the contact name or header to view options, tap 'Disappearing messages', and set a timer.
- The recipient will be informed of the timer set; do the same thing to remove the timer once you don't need it anymore.
- This is useful when sending sensitive information, in particular with HRDAPers at heightened risk, and if you are not sure about the recipient's security level and its device's safety and reliability.

Lost chat history: If you lose chat history or have other issues with Signal you can go here for help;

Safety numbers: Safety numbers allow users to verify privacy of communication with a contact, see here for more info.

Creating Signal groups: If you would like to create Signal groups, such as to communicate with other HRDAPers, you could do so with Signal groups. They work similarly to other platforms, but keep in mind that you cannot expel a participant once they are a member of the group