International Service for Human Rights

# Human Rights Defender Advocacy Programme 2023
# 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, 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.
- 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 informal chats. This can also be used as a secure alternative to Mattermost on the HRDAP 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 for yourself 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. Share this with us if you think we might take further measures.

- *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, online materials and coming to Geneva)?*
- *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 Salomé or one of your coach 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 consent before disclosing any information regarding their identity or work (photo, video social media post, etc). If you have concerns or questions, contact Salomé.
- 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 Salomé through Signal that this email belongs to you. You will not be able to enter the HRDAP Platform until Salomé 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, group and individual coaching** of HRDAPers will be hosted through Zoom.

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

You all have received the Zoom links and invitations, except for the individual coachings, as your coach will contact you to organize those.

Please note that live peer-check-in 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 our paid-professional Zoom by locking 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 if you think you are at risk.

**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