6/ Security and Social Media Use

Things to consider

Social media can be a useful tool in supporting and giving visibility to the work of civil society organisations. As contexts vary widely, it is important to use it carefully and strategically.

- Being **visibly connected to HRDs** and promoting their work via social media can reduce the risks they face, or have the opposite effect and increase risks.
- Social media sites are **not appropriate** for any type of sensitive communication. There are a number of potential risks to communicating sensitive data over such platforms, including:
  - The provider of the website may be obliged or requested by authorities to **hand over user details**, including private messages and 'deleted' content.
  - The regular **changes in Terms of Service** by many social media platforms often lead to changes in the privacy settings available or the defaults, making information previously thought to be 'private' more freely accessible to others.
- **Facial recognition** software is also ever more common on social media platforms, regardless of whether users opt into being openly 'tagged' in pictures or not.
- Private messaging on sites and apps may only be protected with weak encryption.

Protection tactics

- Protect your accounts using **strong passwords and two-factor authentication**, and encourage HRDs to do the same.
- Avoid having or using social media apps on devices which contain sensitive information because they collect information from your device. Ideally, access social media sites via a **privacy-protecting browser**.
- Check the **privacy settings** of the social media sites that you use and make them as private as possible.
- If an HRD wishes to connect with you over social media, **double-check** with them if they are sure they would like to do this.
- Always **ask explicit permission** before uploading any pictures, including of HRDs, to social media platforms, and before tagging them.
- Avoid discussion of any sensitive issues over social media messages and encourage HRDs to use alternative, **more secure methods of communication**. Exceptions could be made to this in cases where secure messaging applications themselves are the subject of stigmatisation or criminalisation by authorities.
- Exercise extreme caution regarding any **links which are shared on pages** or in groups related to political or social movements, especially during times of civil unrest, as these may be malicious.