Do's	Don'ts
DO ensure fair access to information about how to use Social Media safely and securely.	**DO NOT** overload PoCs with legal jargon. Rather, discuss with them clearly and simply the issues about their Social Media activities that may concern them directly.
DO engage community members to develop a better understanding of real and perceived risks on Social Media that can manifest online or offline.	**DO NOT** make perfect the enemy of the good. It is impossible to eliminate all risks but possible to manage risks sensibly, as far as resources allow. Make sure prevention and mitigation measures are in place and risk management is intelligently balanced in relation to the expected gains/ benefits of using Social Media for Community-Based Protection.
DO seek support from UNHCR teams in understanding risk, whether related to digital access, digital engagement, data security and/or data protection.	**DO NOT** make assumptions about the risks communities face. Engage with them directly - especially the active Social Media users - to understand what risks are present and how they are managed (or not).
DO design interventions to prevent, manage, minimize or mitigate risks presented by engaging with communities through Social Media platforms.	**DO NOT** act recklessly with the data of persons of concern. UNHCR has strong policies to protect their data. Complying with the policy and following associated guidance can prevent misuse and abuse.
DO work with partners, including local authorities, ICT security services and Social Media companies, to highlight risks that need to be addressed.	**DO NOT** make a final decision about using Social Media without considering the potential benefits and risks of both engaging and not engaging.