✔ Do's

✕ Don'ts

DO provide private areas and/or channels for F&R and reiterate the confidentiality of the information being shared.
Be mindful of the privacy and data protection challenges of Social Media and ensure private and secure channels are available outside SM.

DO NOT pour all your effort into a single channel. The more channels you connect with, the lower the risk of loss of engagement with a community if access to one fails. Multiple channels will probably be necessary to provide all PoCs with an accessible channel to give feedback.

DO engage with existing F&R systems.

DO NOT wait until the community is frustrated by lack of response to their feedback. Rather, make sure the F&R mechanism is designed to perform its key function of 'closing the loop' in a timely manner.

DO adapt your F&R mechanism to the changing dynamics of the operational context. If necessary, go back to the drawing board and be sure to communicate changes promptly.

DO NOT disregard the influence of the gender or age of staff simply because they are invisible to users. Ensure staff know how to refer any sensitive questions that come in or ask for help if they are uncertain how to handle something.

DO present your aggregated feedback data using data visualization with relevant AGD disaggregation. Show trends to support specific aims, such as course corrections in protection programming.

DO NOT use one type and format of reporting for everyone. Remember that decisions need to be made from feedback received, so always customize reporting to fit the purposes of the identified end-users and the needs of the decision-making process.

DO use PoCs' preferred and trusted channels to close the feedback loop.

DO NOT look only at individual feedback but rather analyze comments over time to identify possible patterns.