Do's	Don'ts
DO make sure all staff knows the referral pathways and how to use them.	**DO NOT** delete messages containing private or sensitive information without contacting the sender and explaining why you removed them.
DO train staff and create monitoring systems for PSEA and child protection, as Social Media is often used by minors.	**DO NOT** assume that just because your page is not intended for minors, they will not access it. The usual safeguarding systems you use offline need to be set up online too.
DO connect with other UNHCR offices in your region or beyond, who may have similar Social Media projects or developed integrated data analysis platforms, before you think about creating your own tool.	**DO NOT** create a bespoke platform. This should be a last resort, only if there is no alternative, and done with HQ to ensure inter-operability with existing systems.
DO connect Social Media projects with offline advocacy, outreach and feedback mechanisms as much as possible.	**DO NOT** assume that Social Media automatically means collecting personal data. In fact you can use SM for protection without collecting any personal data.
DO create workflows and SOPS to connect IMOs with protection staff, so they know what information to exchange, in what situations and how.	**DO NOT** create organizational silos in your Social Media activities and don't restrict SM data management to IMOs.