Risk Table: How to safeguard your digital programmes and activities

This table is about safeguarding and risks of Sexual Exploitation and Abuse and Sexual Harassment (SEAH) in digital programmes and activities. Click here for a tip sheet about digital settings

The table below assumes that you already have developed a digital software. Is a Civil Society Organisation (CSO) creating its own digital platform for a programme? If yes, then you also need to consider safety-by-design principles. You use safety-by-design principles by putting user safety and rights at the centre of the design and development of digital platforms and software. The aim is to anticipate and prevent harm which may occur while using the platform, rather than trying to implement remedies after the harm has occurred (definition adapted from INHOPE webpage – click here).

People who are at higher risk of SEAH and other forms of harm in real life are also, generally, at higher risk in digital settings. Examples of groups who are at higher risk of harm and abuse include women and girls and persons with disabilities. Click here to read about safeguarding and intersectionality (how factors connect or compound to increase a person's risk of abuse).

Note: The word "staff" in the table includes staff and associated staff, volunteers, contractors, journalists and other personnel. The word "participant/s" refers to programme participant/s.

Area of risk	Cause of the risk	How does this relate to the work you do? Potential risk mitigation ideas.
Gaps in software,	Gaps/vulnerabilities in software or security can lead to attacks by malware or ransomware or	* Does your organisation have up-to-date and good quality software, malware and ransomware?

malware, ransomware	phishing attacks (e.g. scam emails, unsafe links etc.). These often aim to gain access to sensitive data. If sensitive data is accessed, it could expose participants and staff to risks of SEAH and other forms of harm.	* Do you ask participants to use a specific software or digital platform on their own device? If yes, you should advise them on how to prevent and keep safe from phishing attacks.
Gaps in privacy and data protection	Risks of SEAH and other forms of harm to participants or staff is increased by: • Gaps in digital privacy by CSOs and partner organisations • Data leakages • Gaps from a lack of quality data protection information or procedures Examples of such gaps include: 1. Personally identifiable information or sensitive data of programme participants is stolen and/or used by others without consent. This may include: • Sharing telephone numbers, e-mails, user IDs of programme participants on social media. • Sharing home addresses/household numbers or other identifiable locations such as schools, child-friendly spaces etc. • Taking and sharing of pictures or videos of	* Are all new staff trained on relevant data policies, including digital privacy and data sharing? * Do you have a data protection policy, and/or digital privacy policy? Do you have related procedures including consent forms and password protection? * Do staff and participants understand the importance of data protection and privacy and related risks in digital settings? * Do participants know how to keep their data safe on the platform they asked to use? * Do staff and participants understand what personally identifiable information is? Do they understand the risks of sharing it? And why it can only be shared with consent? * Do staff understand what consent is and how to get consent? * When participants register for the relevant software or digital programme, do they know what they are consenting to? And do they know why they give their personal data? * Are more than two staff members involved in the digital

	participants without consent. • Sharing marital status, age, sex, disability and health status of programme participants. 2. CSO (unintentionally) gives away or sells data (of programme participants) to companies who use them for advertising/marketing or other purposes. 3. CSO uses the information they have for content sharing and advertising, without consent. 4. Staff upload personal information/data on programme participants onto an unsecured software online. 5. Staff share sensitive information with one another instead of only sharing on a need to know basis. Sensitive data can be personal information, data from investigations, details of reported concerns, etc. This risks that people will stigmatise and judge programme participants. 6. Staff sell programme participants data to fraud / hackers / scammers. Examples of CSO gaps in privacy in Nigeria resulted in:	programme design and delivery? (Tip: it helps when more than one person has oversight and access).

	• Sexual contact/meet up/talk • Sending or soliciting sexual photographs via phone, mail, or in person • Sharing unwanted sexual information via phone, mail, or in person • Using personal details to withhold finances	
Digital setting allows for direct/private/1:1contact between staff and participants or community members.	Staff communicate digitally with other staff or with participants or community members on a 1:1 basis / in private / on a direct basis. For example, using WhatsApp. If there is already a power imbalance in the connection / relationship, meeting in a private digital space can increase the risks of SEAH and other harm. Behaviours resulting from the power imbalance include: - "Grooming". This is when someone builds the trust of someone else *with the intention* of eventually abusing or exploiting them. - "Exploitation". Flattering or giving gifts, money or other forms of bribes could be a way to exploit participants. - "Sextortion". Sextortion is when someone blackmails another person by threatening to go	* Are all staff trained on and regularly made aware of relevant data policies, including digital privacy and data sharing? * Do staff know who are the only staff allowed to communicate digitally directly/privately/1:1 with participants and community members? For example, usually only safeguarding staff and staff helping individuals about a report or disclosure should do this. * Does your code of conduct and / or rules on digital programmes explain how staff and participants are expected to behave in digital settings? * Do participants understand what inappropriate online behaviour is? Do they know what should be reported as a breach of the code of conduct? Do they know how to report something? * Are more than two staff members involved in the digital programme design and delivery? (Tip: it helps when more than one person has oversight and access).* Are there

	public with sexually explicit images and videos. Blackmail could include demanding sexual favours. - Cyber stalking of participants[1]. - Requests for direct meetings offline that could result in harm or abuse. In Nigeria, these meetings have led to rape, kidnapping and death.	content moderators for group communications? (staff or participant)
Lack of digital code of conduct or understanding about appropriate behaviour online	Staff and participants may not fully understand how to interact with one other online. When online, people sometimes dare to behave in a way that would not be accepted in person. People who are *anonymous* online could particularly dare to behave inappropriately. Inappropriate behaviours can be harmful, abusive, discriminatory or harassing. CSOs in Nigeria shared these examples: • Participants who use digital settings / platforms of CSO programmes or communications, e.g. social media platforms have been bullied, harassed or stalked by other participants or by CSO staff.	* Are all staff trained on and regularly made aware of relevant data policies, including digital privacy and data sharing? * Does your code of conduct and / or rules on digital programmes explain how staff and participants are expected to behave in digital settings? * Do participants understand what inappropriate online behaviour is? Do they know what should be reported as a breach of the code of conduct? Do they know how to report something?

[1] The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails (Oxford Dictionary Online).

	• Participants receive/share harmful, hateful or illegal digital content from/with one another or staff. This may include: Child Sexual Abuse Material (CSAM); adult pornography videos; violent, racist, hateful comments to incite physical abuse/harm; Harmful advice (e.g., pertaining to suicide, eating disorders); or information relating to terrorism. • "Sexting" - creating or sharing sexually suggestive nude or nearly nude images aimed at grooming/ harassment/ exploitation.	
Gaps in safeguarding measures in contracts with FSP providers	The staff of financial service providers (FSP) can intentionally delay or withhold financial transfers. FSPs in programmes may support cash transfers or payment for services, If FSP staff delay or withhold, it could result in emotional distress, loss of livelihoods, hunger etc. FSP staff could also use their power to cause harm and abuse, including SEAH. Examples from Nigeria include: • Participants could be at risk for overspending, grooming through financial transactions or fraud and identity fraud due to hacks or scam messages or calls.	*In contracts with financial service providers (FSPs), does the contracting organisation include safeguarding principles? OR * In situations where relevant safeguarding principles cannot be included in a contract, does the organisation know what risks to be aware of with vendor actions and digital platforms? Considerations of risks will depend on the platform type and users. They should include as a minimum General Data Protection Regulation compliance, GDPR (even outside of the EU) and an agreement to delete third party data. * Does the organisation have a clear understanding of what a safe financial process includes? * Does the organisation outline how their staff can interact with participants in digital environments?

	• FSP staff could bully participants into giving them a percentage of their money. For example, they could threaten to remove participants from cash transfer or payment lists unless they pay. • FSP staff could demand sexual favours in exchange for access to finances.	
Safety and SEAH risks of using a digital device in insecure, high-risk locations	The risk of SEAH and other forms of harm is increased if a device is used in insecure, high-risk locations. For example, staff or participants may need to travel alone to a remote / distant location to access signal or to buy data in order to participate in the digital activity. This isolation could increase the risk of SEAH and other harm. Staff or others can also use their position of power or advantage to look at someone's phone. They may gain access to photos, contact information, SMS, etc. which could lead to SEAH or other harm.	* Do staff and participants have digital devices (phones, tablets etc.) that are appropriate for the specific location? * Does the programme design consider location and signal and data access for *all* participants? Is there disability-inclusive software included on the device? * Does the organisation have a chaperone or support system to ensure communication with participants that does not increase harms? *Does the organisation have a security assessment process in place for all activity locations, including digital activities?
General digital literacy and general awareness of	If staff and participants have low levels of digital use and digital literacy**, they might not be able to communicate well, clearly and in a positive way	* Do staff and participants have an understanding of what SEAH and harm online might look like in digital settings? * Do staff and participants know how to behave appropriately online / in the digital programme?

online safety in Nigeria	on digital platforms. Also, if staff and participants don't understand: • How to stay safe online • Why it is important to stay safe online • What the signs of abuse or harm are • What bad online behaviours might be formed / become normalised, and • How to respond if they experience or see abuse online. ** Digital literacy includes: People who have digital literacy can find, create and edit content online. This could include text, audio, images and video content.	* Do staff and participants know how and where to report if they see or suspect SEAH or other forms of harm in a digital setting?
Misinformation	People sometimes share information that is incorrect, uninformed or misleading. They also might make false claims. This could lead staff and participants to behave or act in ways that are harmful or abusive (online or in person). For example, sometimes people share false information about others, or they pretend to be	* Do staff and participants know to figure out if digital content and contacts are "reliable"? That is, is the content factual and are the contacts real people. * Do staff and participants know that it is important to check that information is correct before they share it?

	someone else when contacting someone, or they exaggerate information about themselves.	
Lack of easy ways to report abuse or harm	If we want people to use a platform's reporting channel, it must be easy to use for everyone. It must let the reporter be anonymous.	* Does the platform have a reporting channel that is easy to use for everyone? * Does the reporting channel let the reporter be anonymous? * Does that reporting channel link to the organisation's safeguarding focal point? And to the organisation's reporting response procedures?