Tip sheet

Safeguarding in digital programmes or activities

This tip sheet outlines the risks of Sexual Exploitation, Abuse and Sexual Harassment (SEAH) and other forms of harms, like discrimination or harassment, caused by civil society organisations (CSOs) using different digital environments to deliver programmes in Nigeria. This tip sheet was enriched by consultations with individuals from Yobe, Lagos, Ogun, Bauchi and Borno States. We have also referred to the relevant Nigerian laws on digital engagement and privacy (see list in annex for more information).

Please click here to refer to the accompanying table which outlines some safeguarding and SEAH-related risks of activities or programming in digital settings.

There are many benefits to using digital technology in programmes!

The use of digital technology in programmes can play a crucial role in service delivery, information and awareness-raising campaigns, and as a means of communication and information disclosure. Some examples of the benefits are listed below:

- Cash assistance can reach a broader group of people without disturbing them from their daily tasks.

- Social media platforms can extend the voices, issues and rights of specific individuals and groups of people, bring together like-minded individuals and enable people from different locations to learn and engage with each other for positive change.

- Online education programmes can ensure that children across locations and those who cannot physically attend school for safety, health or other reasons, can continue to receive an education.

- Reporting. Through digital technologies, people anywhere can report concerns, harm or abuse anonymously. Being anonymous can make them feel safer, which means that they are more likely to report. Also, with a digital platform, people can report in their own time and agree what information they feel comfortable sharing.

Digital technology used most in programmes in Nigeria

We have listed the most common hardware and software used in Nigeria programmes:

Hardware / type of device:

- Smartphones or non-android or torchlight phones (in other settings they are called analogue or "dumb phones")
- Laptops
- Cameras
- Drones and other connected objects (sometimes used to gather project success stories)

Software / platform:

- Social media (WhatsApp, Facebook, Instagram)
- Research and engagement tools (e.g., kobobox)
- Financial applications (banking apps etc.)
- Emailing platforms (e.g., Gmail, yahoo mail, outlook etc.)

Note: CSOs may use a digital platform or software that is already developed, or may create their own. Specific considerations of "safety-by-design" are crucial for any platform or software development, but they are not elaborated in this tip sheet. Please reach out to us if this is an area you are interested in exploring further.

Examples of how digital activities are used by CSOs in programmes in Nigeria

1. **Cash assistance/transfer interventions including:**

- Mobile money. Often used to notify people of fund transfers via SMS and to carry out phone surveys for post-distribution monitoring.
- Bank account transfers.
- Vouchers that can be exchanged for goods or services.

2. **Social media platforms (e.g., WhatsApp, Facebook) used for:**

- Information sharing and coordination
- Identifying and locating programme participants and affected populations
- Understanding perceptions, gathering feedback and complaints, including relating to SEAH and other harms and abuses

3. **Online education programmes:**

- Digital platforms are used to substitute or complement classes.
- CSOs use devices (laptops, phones etc) and the internet to teach their beneficiaries or participants.

It is important to note that the use of research tools was identified as a very common use of technology for programming in Nigeria. This is not covered in this document. For more information read **this note** on the safe use of digital technology in monitoring, evaluation and research.

How do people interact in programme digital environments?

The consultations identified that interactions between staff and participants in digital settings are carried out in three different ways:

1. **One-way.** CSO staff give information to programme participants using a digital device and/or specific software, e.g., sharing updates and information through WhatsApp or SMS notifications. In such situations the CSO staff have the participant's data, there may/may not be a general contact point for replies.
2. **Two-way.** CSO staff and programme participants interact using a digital device and/or on a specific software (e.g., two-way engagement, including giving information in research and consultations). In such situations the programme participants may have a general account or personal contact details to communicate with.
3. **Social network.** Programme participants interact with each other, or with staff, using a digital device and/or on a specific software.

Risks of SEAH and other forms of harms when using digital technology in programmes in Nigeria

While digital technology provides many benefits and opportunities for humanitarian and development interventions, it also presents a range of risks. The consultations identified eight main areas which, if not managed, may lead to risks of SEAH and other forms of harm:

1. Gaps in software, malware, ransomware (explained in the accompanying risks table - link here).
2. Breaches in privacy and data protection, this includes the protection of the identity of individuals through name, location and other identifiable details.
3. Private engagement / direct contact between staff and participants or community members enabled through digital engagement. This does not include staff, such as safeguarding staff, who are responding to specific reports or disclosures of SEAH and other forms of harm.
4. General lack of understanding about appropriate behaviour online, which can lead to abuse, discrimination or harassment online and sharing negative or inappropriate content.
5. Gaps in contractual engagement with vendors or third-party organisations.
6. Safety and SEAH risks of using the device in a specific location.
7. Misinformation leading to harmful or abusive actions (that occur in person or online), this may include false information or contacts pretending to be someone that they are not online.
8. Inappropriate or inaccessible reporting channels and associated response procedures.

Please click here to refer to the accompanying digital SEAH risks document which gives a detailed explanation and examples of each of these areas of risk.

When you are identifying and assessing risks, it will be important to consider the below points:

- CSOs should identify and mitigate any risks of SEAH and other forms of harm that are caused by using the device or specific software for their programmes. Some risks are complex and can be hard to identify.
- SEAH and other forms of harm in a digital environment may be caused by staff, other programme participants or someone else (e.g., hackers).
- SEAH and other forms of harm may be caused by staff or participants themselves using unsafe technology (e.g., a virus/malware) and / or by a programme participant's data not being fully protected.

- SEAH and other forms of harm may occur in the digital environment, it may start in the digital environment and actually occur in person, or may move back and forth between settings.
- The device itself, the location in which it is used and who it is used by may also increase risks.
- Generally, people who are more at risk of SEAH in real life are also more at risk of SEAH online. Click here for a resource on intersectionality and safeguarding.
- There will be different risks associated with building your own platform or using an existing platform (where you can choose which features to enable/disable). If CSOs are creating their own digital platform, specific "safety-by-design" considerations will need to be considered.

Ways to mitigate risks of SEAH and other forms of harm in digital activities and programmes

Safe digital programmes =

Safe use of digital devices in each location for each individual +

Appropriate behaviour of all users +

Accessible reporting and appropriate response +

Safe and private software and hardware

Making your digital activities safe requires considering both the human and the technology elements.

Questions to start your risk mitigation process

CSOs need to have organisational safeguarding measures in place that integrate and understand digital environments. While your safeguarding measures will be based on the specific risks related to your programme and the users, you can start by considering the following questions:

- How can we make sure that staff and participants know how to use the necessary hardware / devices or software safely?
- Do staff and programme participants have a good understanding of how to behave appropriately online?
- What policies and procedures on digital safety, information technology and cyber security does my organisation need to have in place?
- How can we ensure quality data protection, privacy and understanding of consent within my organisation?
- What are the digital and in-person reporting options that need to be in place?
- Are digital risks of SEAH considered at the programme design phase (and then updated throughout the programme cycle)?

Making your digital activities safe

We have outlined some ways to ensure you appropriately consider digital activities in your safeguarding measures. **Click here** to refer to the RSH Safeguarding Essentials page for more general

information on safeguarding measures. The accompanying risk table (click here to read it) expands on the core suggestions below and suggests ways to mitigate to specific risks.

Policy and Code of Conduct

- Ensure that your safeguarding policy and code of conduct recognise that activities and communications will occur in digital environments. This includes reflecting the legal environment in Nigeria (see Annex below).
- Provide participants with a code of conduct, especially for safe online communities such as online forums. Clearly identify safeguarding leads and channels for reporting concerns relating to SEAH and other forms of harm.
- The code of conduct should establish basic rules/guidelines for how to engage safely online, including on established social media platforms. Staff and programme participants (where relevant) should be sensitised on the guidelines. A few common points include:
    - Generally, staff and associated staff should not connect with or engage privately with programme participants on social media platforms, especially children (under 18 years). Exceptions include but are not limited to:
        - Safeguarding staff and staff who are liaising with individuals about a confidential matter, specific report or disclosure should continue to liaise privately / 1:1 in the most appropriate digital environment.
        - For any digital engagement with children, e.g. child volunteers, it is best to avoid 1:1 engagement and to have more than one person in the conversation group.
    - Organisations should have a code of conduct for online behaviour. This should apply 24/7 like the standard / in-person code of conduct. Alternatively, the existing code of conduct can include digital behaviour.
    - Use of the following content should be forbidden by staff and on CSO platforms: Child sexual abuse material (CSAM); Pornography; Violent, racist, hateful comments; Harmful advice (e.g., pertaining to suicide, eating disorders); Sexting (creating or sharing sexually suggestive nude or nearly nude images especially of children) aimed at grooming/ harassment/ exploitation; Terrorism; and any identifiable information about an individual that you do not have consent to share.
- CSOs should appoint a safeguarding focal point or "moderators" on digital platforms, including social media, that are used to ensure that engagement and communications in the specific platform / digital environment remain appropriate and in line with the code of conduct.
- Ensure the moderators are aware of the policy for handling images and personal narratives online (particularly of children and survivors of SEAH). This should include information that ensures the safety, consent and anonymity of participants.

Device and platform management

- Where possible, use an organisational device to communicate with programme participants. Also, use accounts that have been authorised by your organisation to communicate with programme participants. Ensure any private accounts or devices are authorised.
- Save and keep a record of communications with programme participants, especially when using (organisationally authorised) private channels.
- When setting up the platform, ensure that decisions regarding what features to enable / disable consider the safety of the online participants. For instance, restrict access to accounts engaging young participants and filter content to remove abusive content through keywords and phrases.

Risk management

- CSOs should develop a risk register or summary document on the risks of SEAH and other harms that can be encountered in the different digital environments they use. Risks will change over time so regular risk reviews should be undertaken.
- Additional risk assessments should be made when engaging with third-party digital service providers (e.g., data collectors, Financial Service Providers (FSPs)) and develop a mitigation plan to address the potential risks.

Click here to refer to the accompanying, more detailed, digital SEAH risks table.

Training and information awareness to staff

- It is important that all staff are aware of the risks of engaging online so that they can help identify, mitigate and also respond appropriately should they witness or suspect abuse or harm online in a digital activity they are working on.
- Training or information awareness on the opportunities and benefits of engaging online as well as the challenges and risks of SEAH and other harms online is key. Other aspects of harm may include inaccurate information, or "fake news", with potential to cause conflict or visuals that give prominence to perpetrators or their ideas.
- Training should include content on cyber security and phishing/hacking/spam, laws relating to privacy and abuse online (see annex below), disinformation, online kindness and behaviour, data protection and privacy and reporting procedures (online and in-person).

Information awareness to programme participants

- If CSO programme activities require participants to engage in a digital environment, the CSO will be responsible for any harm that occurs to a programme participant in that digital setting, even if it is between participants.
- As with staff, programme participants should receive training and information awareness on the opportunities and benefits of engaging online, as well as the challenges and risks of SEAH and other harms online. Information can be categorised into:
    - Disinformation and 'fake news'. This content has the potential to cause conflict, tensions or harm, including to cause SEAH. It may also give prominence to perpetrators or their ideas, which could lead to harm including SEAH (online or in-person).
    - Privacy and security. This includes content on cyber security and phishing, hacking and spam, information on laws relating to privacy, data protection and abuse online (see annex below).
    - Online safety. This includes information on online kindness, appropriate online behaviour, how to identify abuse, including SEAH, online. It should also include information on reporting procedures (online and in-person).

Hardware and Financial Considerations

- To curb the risk of personal data sharing, organisations should design their programme to include a budget for buying digital phones, laptops and cameras. This is to mitigate the personal use of phones by organisation staff to store programme participant's data.
- Organisations should install cybersecurity measures such as anti-virus and network restrictions for inappropriate sites on work laptops and devices.
- Organisations should have clear Data Protection or Data Management policies and procedures so staff know where to store personally identifiable information safely.

We are always learning! As you begin, continue or expand your digital activities please do email the RSH in Nigeria to share safeguarding-related challenges and successes.

Annex – Relevant Laws and Standards on Digital Engagement and Privacy in Nigeria

NITDA REGULATION. The NITDA Act empowers the National Information and Technology Agency (NITDA) to issue guidelines to cater for electronic governance and monitoring the use of electronic data exchange.

Deriving from this provision, NITDA then developed and issued the Nigeria Data Protection Regulation 2019.

THE 1999 CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA. The Constitution of the Federal Republic of Nigeria 1999, as amended ("the Constitution"), which, by virtue of section 37 thereof protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication. Data privacy and protection are thus extensions of a citizen's constitutional rights to privacy

FEDERAL REPUBLIC OF NIGERIA CHILD RIGHTS ACT (2003). Section 8 of the CRA which covers a child's rights to private and family life states that a child is entitled to his privacy, family life, home, correspondence, telephone conversations and telegraphic communication.

FREEDOM OF INFORMATION ACT 2011(FOIA). Section 14 of the FOIA limits Government agencies from disclosing the personal information of citizens unless the individual's consent is obtained, or the information is publicly available.

CYBERCRIMES (PROHIBITION, PREVENTION ETC) ACT 2015 (CPPA). The fundamental purpose of the CPPA is to establish a framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It imposes an obligation on mobile networks, computer and communications service providers to store and retain subscriber information for a period of two years.

CENTRAL BANK OF NIGERIA CONSUMER PROTECTION FRAMEWORK 2016 (CPF). The provisions of section 3.1(e) of the CPF are to the effect that consumer information must be protected from unauthorised access and disclosure. In order to enable disclosure, financial services institutions are required to obtain written consent of customers before their data may be shared with third parties or for promotional purposes.

THE CREDIT REPORTING ACT 2017 (CRPA). Section 9 of the CRpA is to the effect that Data Subjects i.e., persons whose data are maintained by credit bureaux, shall be entitled to the privacy, confidentiality and protection of their credit information subject to certain exceptions listed under section 9(2) to 9(6) of the CRpA.

THE NIGERIA COMMUNICATIONS COMMISSION (REGISTRATION OF TELEPHONE SUBSCRIBERS) REGULATIONS 2011 (NCC REGULATIONS). Regulation 9 of the NCC Regulations specify that, in

furtherance of the rights guaranteed by section 37 of the Constitution and subject to any guidelines issued by the NCC or a licensee, any subscriber whose personal information is stored in the Central Database is entitled to request updates; to have the data kept confidential

References

Adegoke, A., 2020. *Digital Rights and Privacy in Nigeria,* Abuja, Nigeria : The Paradigm Initiative.

CentruyLink , no date . *Tips for email safety.* [Online]
Available at: https://www.centurylink.com/home/help/internet/security/tips-for-email-safety.html
[Accessed 13 July 2022].

Elluard, C., 2015. *Guidance Notes: Cash Transfers in Livelihoods Programming- West Africa.* [Online]
Available at: https://www.calpnetwork.org/publication/guidance-notes-cash-transfers-in-livelihoods-programming-west-africa/
[Accessed 06 07 2022].

Federal Republic of Nigeria , 2011. *Federal Republic of Nigeria Official Gazette,* Lagos, Nigeria : The Federal Government Printer .

Federal Republic of Nigeria , 2019. *Federal Republic of Nigeria Official Gazette,* Lagos, Nigeria : The Federal Government Printer .

Federal Republic of Nigeria, 2007. *Federal Republic of Nigeria Official Gazette,* Lagos, Nigeria: The Federal Government Printer.

LawNigeria , 2018. *Constitution of the Federal Republic of Nigeria 1999 (with amendments).* [Online]
Available at: https://constitution.lawnigeria.com/2018/03/26/1999-constitution-with-amendments-nigerian-constitution-hub/
[Accessed 15 July 2022].

Lüge, T., 2017. *How to use social media to engage with people affected by crisis.* [Online]
Available at: https://www.icrc.org/en/document/social-media-to-engage-with-affected-people
[Accessed 01 July 2022].

Lunt, A., 2017. *Messaging apps: the way forward for humanitarian communication?.* [Online]
Available at: https://medium.com/law-and-policy/messaging-apps-the-way-forward-for-humanitarian-communication-74ab8f3b113e
[Accessed 18 July 2022].

Overseas Development Institute, 2015. *Doing cash differently: how cash transfers can transform humanitarian aid.* [Online]
Available at: https://odi.org/en/publications/doing-cash-differently-how-cash-transfers-can-transform-humanitarian-aid/
[Accessed 17 July 2022].

Privacy International, no date. *Expose Data Exploitation: Data, Profiling, and Decision Making.* [Online]
Available at: https://privacyinternational.org/old-our-interventions/expose-data-exploitation-data-profiling-and-decision-making
[Accessed 05 July 2022].