

# SAFETY AND SECURITY GUIDANCE

# HOW TO PLAN FOR SAFETY AND SECURITY WHEN IMPLEMENTING ACTIVITIES WITH KEY POPULATIONS

This guidance is for REAct Coordinating and Implementing Organisations and others working with key populations in environments where those populations are highly stigmatised and criminalised, and where their safety and security could be at risk, not only in their daily lives, but also when they report human rights violations, get referred, and agree to have their stories told to contribute to advocacy efforts. It is important to remember that when we work in these contexts promoting the rights of stigmatised and criminalised groups, we run the risk of unintentionally causing harm to those we wish to help, as well as ourselves - staff, outreach workers, volunteers- and our fellow civil society communities. Our first responsibility is to do-no-harm: make sure that we do everything we can to ensure that the individuals who report violations, and the people who work on these issues are safe. If at any point our work has the likelihood of putting people ate risk of harm by our work, we must not proceed, no matter how important we may feel our work is. Therefore, we must make sure that we are aware of the safety and security risks that we and others may face, and have strategies at hand to prevent – and respond - effectively to safety and security risks in the course of our work. We all need to learn from incidents that have occurred, during which and clients experienced fear, harassment, arrest, eviction, discrimination and violence while working with key populations – sometimes as a result of identifying as a member of a key population ourselves.

We must make sure we do everything that we can to protect the data, and to make sure that clients who report are fully aware of the implications of reporting, and give informed consent to how their data will be protected, used, or not used. We must make sure that our referrals are to organisations and institutions that we know will also practice do-no-harm principles.

This guidance, which is focused on programming, complements organisational strategies and policies. It supports those who are implementing activities with key populations. It does not replace or override existing organisational security, 1 child protection or risk management strategies or policies.

Please consider each of the recommended steps within your country context as they may not always be appropriate or practical.

#### **KEY RECOMMENDATIONS**

- Each organisation should conduct a comprehensive security assessment, and develop and implement strategies and policies to ensure the safety and security of staff, outreach workers, volunteers and clients.
- Each project should develop and operationalise an emergency response plan and budget that includes communication channels and decision-making processes.
- Significant time and resources should be invested in training all staff, outreach workers, volunteers and clients on their personal safety in the field.
- Safety and security should be built into all project-related trainings, such as peer educators' trainings, community mobilisation trainings and healthcare provider trainings.

This guidance provides practical advice for staff, outreach workers and their clients on how to plan ahead and prepare for potential incidents when working with key populations. It aims to support individuals to be able to take quick and decisive action to prevent or minimise the likelihood of injury to themselves and others. This guidance is broken down as follows:

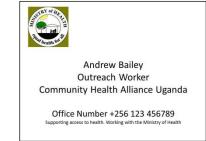
<sup>&</sup>lt;sup>1</sup> Organisational security involves country-context risk assessment and review of existing organisational, office and ICT security plans.



- Practical steps for organisations
- Additional steps for individuals
  - o In the office
  - o In the field
  - Safety of clients
- Useful tools
  - Organisational checklist
  - o Exercise: What would you do if ...?

#### 1. PRACTICAL STEPS FOR ORGANISATIONS

- Nominate a security point person in your organisation. Their role is to explain to colleagues, and regularly
  remind them of, organisational policies and procedures, as well as programmatic emergency response plans
  and protocols. This person would receive training and guidance. When there are concerns about safety issues
  or when incidents occur, they would not make decisions on their own but would bring these to the
  team/organisation for discussion.
- Identify a clear decision-maker and decision-making process for different types of incidents (e.g. a security point person, and the next designated decision-maker).
- Make a phone tree for all staff and outreach workers (especially if the organisation is large) so everyone knows each other and who to contact for what purpose.
- Develop a relationship and agreement with a lawyer, law firm or AIDS Legal Network for when advice or support is required. In addition, if possible, train advocacy officers to provide basic legal information and support. It is preferable if your organisation understands its rights, and possible actions to take, ahead of any incident.
- All staff and community outreach workers should be issued with ID cards stating their name, organisation, job title, and the telephone number of the office or a manager. Speak to a well-accepted partner (e.g. a ministry of health) about putting a statement (e.g. 'This project is supported by the ministry of health') or their logo on the card. A logo is a good idea in cases where people might recognise an image but cannot read a particular language.
- When working with young key populations, there are important additional considerations. Staff and community outreach workers need to know their country's laws and policies when providing services to children and young



A sample ID card

- people (e.g. age restrictions and the need for parental consent to provide an HIV test and contraceptive services). It is important to be aware of social attitudes around sex, gender identity, sexuality and drug use when providing services to young people. Staff and outreach workers must clearly understand the strategies and approaches used in their project, and confidently articulate the services they are providing and the partners they are working with. They also need to know the name of a contact person should further questions arise.
- Map where your organisation is working, the closest safe zones and how to get to them. This includes identifying and having contact details of friendly partners and colleagues (e.g. police, clinicians, priests, imams and other community leaders) who can help when needed.
- All staff and community outreach workers need to know their ICE (In Case of Emergency) numbers and to have it in their phones.
- All staff and community outreach workers need to read their organisational security policies and sign that they
  have read and understood them.
- Staff should have regular safety and security discussions during their meetings. All staff must understand procedures, and update any contact lists they use. Staff teams should regularly reassess risk threshold levels, as this will determine, for example, whether to 'keep a low profile' or 'speak out'.
- Staff and outreach workers need to document incidents and follow-up actions in a log book, and review these during meetings for learning purposes.



- Staff and outreach workers must use pictures with care on Facebook or other social media (do not tag colleagues or others without their permission). Also be careful about sharing your location or particular activities, especially a location you visit or an activity you conduct regularly.
- All staff and outreach workers need to be clear when dealing with the media (both in negative and potentially supportive circumstances), and should know who to refer questions or requests for interviews to.
- All staff and outreach workers need to speak clearly and consistently about the 'access to health' work they
  are carrying out. If colleagues describe their work inconsistently this can be problematic. Also, be cautious
  about when and how to use human rights language.

#### WHERE THE RISK THRESHOLD IS HIGH

- Set up a security rapid response team to support the security point person.
- Implement strategies from the comprehensive security assessment.
- Install alarms and/or security guards for the office. Ensure that new staff members are well briefed and supported so they can act in the best interests of the organisation.
- Where security incidents are likely to occur, an organisation can choose (for example) to:
  - advise staff to work from home
  - o work in a virtual office, perhaps housed in a partner's office
  - rebrand.
- Identify friendly partners and allies for updates on the security situation, including local United Nations offices and donors.
- Consider identifying safe houses in emergencies for a few staff members at a time, for a few days, when they cannot return home.



#### 2. ADDITIONAL STEPS FOR INDIVIDUALS

These steps are advised for work contexts, but they could also be appropriate for some staff, outreach workers and clients in their social contexts and communities.

#### IN THE OFFICE

- Be aware of your regular journeys, including routes and times, between home and office (especially if your office or centre is well known).
- Be clear about safety in the office. For example, do you need to sign in? Are visitors only welcome by appointment? Who controls how visitors enter the building a receptionist or anyone at all? Who monitors who is in the office?
- Be aware of the posters and leaflets you have around. For example, if you have MSM pictures and information displayed on the wall, might these get you into trouble if your office is raided?
- Encrypt sensitive data on your computer or back up documents on your Google drive.
- Escalate threatening emails or phone calls to your security point person. Calls needs to be logged and discussed with the team before you decide whether and how to respond.
- If you feel unsafe working in the office, speak to your security point person about your concerns. They might suggest you could consider working from home.



Set up a Whatsapp group or similar group messaging function via mobile phone to connect an outreach team or any group working together with key populations. In an emergency, one message goes out to everybody.



#### IN THE FIELD

# **BEFORE GOING TO THE FIELD**

- Make sure that your mobile phone is fully charged, and that your next of kin, In Case of Emergency (ICE) and local contact numbers are on it. Make sure you have airtime.
- Make sure you have your ID card with you.
- Where possible, travel in pairs.
- Make sure you know where you're going. For example, do you know the area well? Do you understand your political context and environment? How will social attitudes affect you when, for instance, working with young people on issues to do with sexuality, gender identity, sex work and drug use? Have you negotiated a particular time and safe space to meet with clients?
- Identify your personal safe zone in an emergency.
- Be clear about the friendly contacts (police, clinicians, community leaders) you would get in touch with for updates or in case of a threat. Remember, a friendly contact for one key population may not be so friendly for another key population. Also, opinions and views change over time: ask colleagues for advice and keep up to date.
- Agree with a manager how often and how you will check in.
- Consider how you will travel. For example, do you have transport money?
- Be aware of the possible consequences of your appearance, such as how you dress, so you do not attract unwanted attention, especially when working in hostile environments.

#### **DURING YOUR TIME IN THE FIELD**

• Check in with your manager at the times you have agreed (e.g. at the end of each day).

#### **AFTER BEING IN THE FIELD**

 Make sure you let your manager and the security point person know when you're back (e.g. write it on the board, send an email), share or log any security incidents or near misses that occurred, revise your outreach spots.

Every effort needs to be made to ensure that all staff and outreach workers feel comfortable about their work in the field. This is particularly important for young peer educators and outreach workers, who may have less experience of working in the field. In some cultural contexts, they are likely to be especially vulnerable to negative social attitudes, questioning or aggression because of their age.



# **Safety of clients**

Below are some suggestions for clients. This information can be included in a flyer to give to clients to remind them to stay safe.

#### **BEFORE GOING TO THE FIELD**

- Be over-cautious if you feel threatened or in danger only go to places where you feel safe or contact a friendly person who can help you.
- Be clear about why you're attending an outreach session or meeting an outreach worker so you're ready to face questions from friends, neighbours or colleagues (e.g. for a 'health education session').
- Make sure you have your next of kin and In Case of Emergency (ICE) contact numbers on your phone, and make sure your phone is charged and that you have airtime.
- Be aware of the possible consequences of drawing unwanted attention to yourself through your appearance (e.g. the way you dress).
- Remember not to check in on Facebook saying where you are if it may lead to danger.

#### SWEAT/SISONKE CARDS 'MY RIGHTS WHEN DEALING WITH THE POLICE'





I have a right to contact and speak to my legal adviser before I say anything to you. I need to use a phone to do that, and can phone a mobile if necessary. Please do not ask me questions until I speak to them.

I do not give you permission to search me.

I have a right to be free from violence, and to be treated with respect by you and all other officers. That includes a clean cell and blenkets, meals and medication (Police Standing Orders G341, 349 (2), 361).

I want to be released without delay. I have a right to apply for police bail and wish to exercise that right.

Thank you for respecting my rights.

Please contact The Human Rights Defence Team (SWEAT, Sisonke and Women's Legal Centre) if you need more information. The number is 076 3112 543



# 3. USEFUL TOOLS

# **ORGANISATIONAL CHECKLIST**

|   | Yes | No |
|---|-----|----|
| Do we have an organisational safety and security policy?  |     |    |
| Do we have a programmatic emergency response plan?  |     |    |
| Do we have a child protection policy when working with children and young people?   |     |    |
| Do staff members understand the organisational safety and security policy?  |     |    |
| Have we set aside a budget for safety and security (e.g. in case we need legal support)?  |     |    |
| Do we know how to access that budget (e.g. who to ask if we need to pay for something security related; who to ask for money if the budget-holder is away from the office)? |     |    |
| Have we nominated a security point person?  |     |    |
| Have we identified a decision-maker and decision-making process for different types of incidents?   |     |    |
| Do we have a working relationship with a lawyer, law firm or AIDS Legal Network for advice or support when required?  |     |    |
| Do we have a list of emergency contacts, such as our lawyer, or a supportive ministry of health or United Nations person?   |     |    |
| Do all staff and outreach workers carry ID cards?   |     |    |
| Do all staff and outreach workers map where they are working, the closest safe zones and how to get to them?  |     |    |
| Do all staff members know what to do in case of a safety and security emergency?  |     |    |
| Do we hold safety and security discussions during staff meetings?   |     |    |
| Have staff members discussed how to use Facebook safely (pictures/tagging/location)?  |     |    |
| Do all staff members know how to talk clearly and consistently about their work (the 'one-line pitch' about what we are doing)?   |     |    |



# **EXERCISE: WHAT WOULD YOU DO IF...?**

Discuss each of the scenarios below in your team. Then act them out (or use your own actual examples of difficult situations). Note your team's responses.

Work together to identify the kinds of threats and where they might come from in your own context (including people who have been threatening in the past).

| Examples   | What to do |
|--|------------|
| What happens if an angry government official turns up at your office?  |            |
| What happens if your outreach worker is arrested?  |            |
| What happens if the police raid your office?   |            |
| What happens if you receive a call from a peer educator saying they don't know where they are or they are in trouble, and then their phone cuts off? |            |
| What happens if your client is beaten up?  |            |
| What happens if an angry parent shows up with a crowd at your office and accuses you of turning their son gay?                                       |            |
| What would you do if the media puts a negative article in the newspaper showing the location of your office and a photo of your peer educators?      |            |
| What if one of your clients puts up photos of the latest outreach session on Facebook?   |            |
| What happens if a transgender colleague is detained at the airport and their passport confiscated?   |            |