EUROJUST
European Union Agency for Criminal Justice Cooperation

Network for investigation and prosecution of genocide, crimes against humanity and war crimes

Cour Pénale Internationale
International Criminal Court

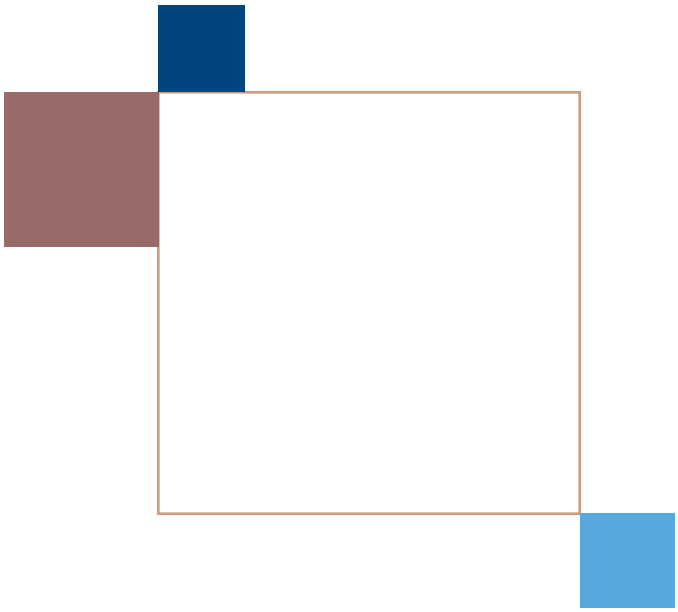
Le Bureau du Procureur
The Office of the Prosecutor

# Documenting international crimes and human rights violations for accountability purposes:

## Guidelines for civil society organisations

# Table of content





# FOREWORD

These guidelines will reach you at a time when international peace and justice are under severe pressure. We continue to see the profound impact of armed conflict and the commission of atrocities across the globe, with the situation in Ukraine again underlining the essential need for all actors to work together to demonstrate the relevance of international criminal justice to the lives of those affected by such crimes.

This moment, however, has also given rise to renewed and global support of action toward accountability for core international crimes and human rights violations. It is encouraging us to build partnerships and, in recent months, we have taken steps to further strengthen cooperation between the Prosecutor and Eurojust. The joint issuance of this publication is a further demonstration of our personal commitment to work together in this common effort.

The fight against impunity is not solely the preserve of States or international organisations. It is a collective obligation that must benefit from the contribution of all those who seek to advance the cause of justice. Civil society organisations are critical to this common work. Across situations globally, we have seen how civil society actors are increasingly active in documenting core international crimes and human rights violations, demonstrating an ability to make crucial contributions to accountability efforts.

These guidelines are intended to further assist you in your efforts to collect and preserve information that may ultimately become admissible evidence in court. They provide some key principles which, we believe, may be of assistance in ensuring that documentation efforts are carried out in a way that preserves the integrity of information and evidence and increases the ability of national and international accountability processes to draw on your work. Our cooperation should continue even in relation to these guidelines. This should be a living document that we further improve and build on based on our future work together.

As prosecutors, we have both experienced first-hand how criminal proceedings play an important role in recognising the suffering of victims, and how the confidence that justice has been served greatly contributes to restoring their dignity. It is critically important that victims are both seen and heard in the accountability process. We have also seen that meaningful accountability can only be achieved by working together, by drawing on the contributions of all those who seek to fight impunity.

We take this opportunity to thank you for the important work you are undertaking. Together, we will strive to create a global culture of accountability that will help to restore justice, rebuild societies and educate future generations. In doing so, we will seek to deliver on the promise of international justice, where the value of all lives is recognised. Humanity deserves no less.

Karim A. A. Khan QC
Prosecutor of the International Criminal Court

Ladislav Hamran
President of Eurojust

# 1. INTRODUCTION

Civil society organisations are important partners for national authorities and international accountability mechanisms in our collective pursuit of justice for international crimes.

The present guidelines have been developed jointly by Eurojust, the EU Network for investigation and prosecution of genocide, crimes against humanity and war crimes ('Genocide Network') and the Office of the Prosecutor of the International Criminal Court. They are addressed to civil society organisations in support of their independent efforts to preserve and collect information on the commission of international crimes and human rights violations for accountability purposes. In particular, the guidelines address how such efforts may best be directed when they are intended to assist criminal accountability processes, such as those before national courts or the International Criminal Court ('ICC').

This is not a manual. Rather, it sets out a series of proposed 'do's and don'ts' from the perspective and advice of national investigative and prosecuting authorities and the Office of the Prosecutor of the ICC – both on what may help and what could potentially harm criminal accountability efforts. The aim of these guidelines is to ensure the most effective channelling of efforts and capacities towards the common objective of combatting impunity for such crimes.

In this context, multiple civil society organisations and stakeholders in the accountability field have expressed a need for guidance to support them in ensuring that the information they collect can support the efforts of the competent investigative authorities[1] and potentially be used as evidence in future prosecutions at the national or international level.

## Who should use these guidelines?

This document is specifically addressed to civil society organisations. These include organisations that undertake efforts to document international crimes and human rights violations, with the purpose of handing over information to accountability mechanisms. In this context, the term includes both those organisations that pursue accountability efforts as their primary mandate, and those that have other purposes but also take actions to preserve information for accountability purposes.

These guidelines have not been designed for competent investigative or prosecutorial authorities, meaning those investigations that are led under a legal mandate related to a national or international judicial accountability mechanism for whom different considerations may apply.

It is also to be noted that these guidelines, while useful, do not apply to those who provide legal services to victims, other persons or entities, including acting as their legal representatives in national or international proceedings (administrative, civil and criminal, e.g.).

## Scope and purpose

The documenting activities of civil society organisations have proven invaluable to accountability efforts. The work conducted by such entities is typically carried out under highly challenging circumstances and will often represent the first engagement by documenters on the ground, before engagement by competent investigative authorities.

The timely access by civil society organisations to information and affected communities, combined with their collective expertise and their ability to swiftly share information, places them in a privileged position to support the activities of competent investigative authorities. They may do so by collecting information that may otherwise be lost, and by accessing, verifying and analysing information, including documentary information, electronic information and online materials. As such, civil society organisations are encouraged to share any information and analysis relevant to international crimes and human rights violations with the competent investigative authorities as soon as possible, in line with their independent activities.

Eurojust, the Genocide Network and the Office of the Prosecutor of the ICC acknowledge that in some instances, competent authorities may not be willing or able to exercise jurisdiction to provide criminal accountability. In such cases, civil society organisations might decide to pursue other avenues for accountability, while preserving information and material collected for potential use in future criminal accountability efforts.

[1] This term includes any national, hybrid or international institutions (governmental, intergovernmental or international) carrying out criminal investigations.


However, there are also limits to what may be useful. Some activities conducted on the ground also have the potential to be harmful or prejudicial to criminal accountability efforts. Clearly, civil society organisations cannot replace or substitute the actions of competent investigative authorities mandated to enforce the law. As reflected in lessons-learned exercises conducted by civil society organisations themselves, experience has also shown that, at times, well-intentioned documentation efforts by civil society organisations have the potential to be counter-productive for the purpose of supporting accountability mechanisms if they do not align with key standards. For instance, the repeated comprehensive interviewing of the same individual can affect the safety and well-being of the person and also detrimentally affect the evidence that the person may be able to provide.

The presence of multiple civil society organisations and stakeholders in the same accountability sector using different standards and tools also gives rise to the risk of over-documentation, increases the risk of re-traumatisation and has the potential to compromise the quality of evidence ultimately available for accountability purposes. These guidelines are intended to support civil society organisations in their work and ensure the safety and well-being of persons providing information.

These guidelines build upon similar products that have previously been developed by civil society organisations themselves[1]. They therefore seek to consolidate and enhance existing efforts already undertaken by civil society organisations to ensure their work is carried out effectively and in accordance with international standards. Where not already doing so, civil society organisations that conduct efforts to document international crimes and human rights violations are encouraged to reflect these guidelines in their standard practices.

These guidelines are intended to be a dynamic document that will be updated to reflect the experience of civil society organisations and in consultation with them.

## Responsibilities of civil society organisations

These guidelines are not intended to – and do not – direct, mandate or solicit civil society organisations to take any action on behalf of Eurojust, the Genocide Network, the International Criminal Court or other accountability mechanisms. Therefore, the independent activities of civil society organisations cannot be attributed to them.

It follows that civil society organisations remain, at all times, responsible for their own conduct, including with regard to both their own physical safety and any potential liability under applicable laws, especially with regard to the legislation of the country in which they are operating. Consequently, civil society organisations should, in their own interests, endeavour to comply with any applicable national laws at all times.

[1] See 'Key resources' in Annex 4.

# 2. GENERAL PRINCIPLES

## Do no harm

Civil society organisations should seek to prevent or minimise any unintended negative effects of their documentation activities on others and themselves. Such activities should always be conducted in the best interest of persons providing information, intermediaries, local communities and any other person involved in the documentation process. Their security, physical and psychological well-being, and privacy should be prioritised during the documentation process, and activities that expose the above persons to a risk of harm should not be undertaken. This entails conducting several actions prior to, during and after documenting, such as carrying out risk assessments, training and selecting staff to ensure professional standards of conduct, obtaining informed consent, protecting sources, respecting confidentiality, setting up referral support systems, and paying particular attention to and applying specific measures when dealing with vulnerable persons[1].

Documentation activities should be carried out in a manner that contributes to and does not negatively impact future evidence collection or accountability efforts, including eventual prosecution of perpetrators of core international crimes, by official national or international authorities. Even well-intentioned efforts to collect information for use in accountability processes have the potential to detrimentally affect the usability of the information as evidence in future proceedings. This applies, in particular, to the questioning of persons.

Where work is conducted primarily to support future criminal investigations by competent authorities, civil society organisations should seek to avoid taking detailed accounts from persons about their knowledge of crimes. Instead, priority should be given to identifying the topics that a person could speak about and recording the contact details of the person to facilitate a future interview by the competent investigative authorities. This information should be preserved with a view to pass it on to competent national or international investigative authorities, such as the Office of the Prosecutor of the ICC, at the earliest opportunity.


[1] See Section 4.

## Informed consent

Prior to any information-gathering exercise involving other persons – such as questioning a person, taking photos/videos, receiving documents – **civil society organisations should obtain the informed consent of the person or entity with which they engage**.

To strengthen the potential use of information collected from individuals in future criminal proceedings, when seeking to obtain consent, consider using the template in Annex 1, as well as ensuring activities are carried out in line with the following guidelines.

- **Consent must be *informed*:** The person must be given a full explanation of the nature and purpose of the activity, the procedure that will be followed, the potential use of the obtained information (including potential publication or applicable legal requirements) and the foreseeable consequences of sharing information, including potential security risks. Efforts should be made to adequately provide and explain to the person all the relevant information, and to evaluate the person's ability to fully understand what is being presented in order to provide a valid consent.
- **Consent must be *contemporaneous*:** Renew the person's informed consent to cooperate in an information collection activity on an ongoing basis, as it can be withdrawn at any time. Consent for the information provided to be shared with national authorities, the Office of the Prosecutor of the ICC or other international accountability mechanisms can be withdrawn until the information is actually shared.
- **Consent must be *voluntary*:** Respect the free will of the person. Ensure a non-coercive environment and empower others to express their views freely. Be mindful of social contexts that might inhibit the person's ability to freely consent to the activity, such as culture-, gender- or age-related dynamics, community or family pressure. Expressly inform persons that up until the time when the information is shared with the competent national or international authorities they can change their mind and decide not to cooperate.
- **Consent must be *explicit*:** Whenever possible, produce a record of the provision of informed consent. Such record can be in the form of a written record signed by the person providing consent, an audio/video recording or any other means, as long as it clearly identifies the person providing the consent and includes the following: the information provided on the nature and purpose of the documentation exercise, on the associated security risks and on the intended use of the information; any terms as to its confidentiality; an express statement from the person that the consent provided is voluntary; and any other information relevant to the voluntary consent.

When seeking a person's consent, also ask the person for their informed consent to share the information obtained with any competent national or international investigative authorities, such as the Office of the Prosecutor of the ICC.

In that context, where assessed appropriate, inform the person that the competent authorities will maintain the confidentiality of the information subject to applicable rules, which may vary depending on which national authority is exercising jurisdiction. Inform them also that the information may be shared with any parties in potential judicial proceedings, including the defence. It is also important to manage the person's expectations as they may not necessarily be contacted later by such authorities. Do not make unrealistic guarantees or promises about the future use of the information collected or any potential benefits. If required, discuss different modalities for sharing information (for example, providing both the information and biographical/contact details or just anonymised information).

Reflect the informed consent for sharing the information on the informed consent record, including **any** concerns raised or conditions placed to the sharing of information. Consider using the 'Informed consent template' (Annex 1) and, if necessary, assist the person in fully understanding and completing the informed consent template.

Once you have obtained the informed consent of the person for the information to be shared, securely preserve the information received with the view to provide it to competent national or international investigative authorities at the earliest opportunity. If sharing information with multiple jurisdictions, inform each jurisdiction to facilitate coordination.

## Objectivity, impartiality and independence

In line with their independent activities, civil society organisations should seek to ensure their actions are carried out in an objective, impartial and independent manner, consistent with the collective aim of discovering the truth. These efforts will be strengthened by carrying out work in line with the following principles.

- **Objectivity:** Seek to establish the truth; do not make assumptions; consider both incriminatory and exculpatory information equally; consider multiple hypotheses and theories and review them; plan your activities on an ongoing basis as information is collected; do not influence information providers (e.g. by using leading questions); do not apply legal assessments when gathering factual information (e.g. enquiring on whether an attack was 'indiscriminate'); evaluate sources of information and review the collected information to test its reliability.
- **Impartiality:** Do not take sides; remain unbiased and unprejudiced; be aware of your cultural and personal biases; implement working methodologies that cover all relevant facts and information and take proactive measures to prevent 'tunnel vision' or 'confirmation bias'; identify and avoid any conflicts of interest.
- **Independence:** Exercise your activities free from any interference, influence, or the presumed or known wishes of any person or authority. Be aware of any organisations or individuals manipulating information or putting out false information to undermine documentation efforts.

## Accountability and legality

In conducting their work, members of civil society organisations should be aware that they do not benefit from any immunity or privilege associated with an official accountability mechanism with whom they may share information. Nor do they act at its direction or on its behalf. To support the integrity of information collected and protect the rights and well-being of their staff members, civil society organisations should:

- be mindful of potential liability under applicable laws, especially in the country in which they are working;
- be mindful that representatives may potentially be called to testify in any subsequent proceedings in relation to information collected by them, for instance to outline the activities, methods and procedures of the organisation;
- maintain a detailed record of their methods and procedures to preserve and collect information, and apply sound information management practices. In so doing, ensure that the information contained in this record is kept confidential and secure (for example, use coded language or save the record in an encrypted device, if required).


©International Criminal Court

## Professionalism and respect

To further strengthen the potential use of information collected through their activities, civil society organisations should seek to:

- always act with professionalism, integrity, respect and empathy, and be mindful of cultural sensitivities and vulnerabilities. Be aware of the possible impact of their conduct on those with whom they interact;
- never pay or offer any form of remuneration in exchange for information; define in advance the conditions and criteria where support to persons participating in the documentation process is to be provided (e.g. payments of transport; food during meetings; expenses related to security and protection); keep a record of all payments made and their justification.

# 3. PLANNING AND PREPARATION

Thorough planning and preparation of any activities intended to preserve and collect information is key. To that end, civil society organisations should consider the following:

## Early preparation

**Research the operational environment:** Consider the type(s) of alleged criminality, the parties involved and the potential perpetrators, the vulnerability of the population, the socio-cultural, political and religious context, gender, age, as well as applicable legislation relevant to the documentation activities.

**Define your mandate, objectives and focus:** Define what you are documenting and for what purpose. Determine the geographical and temporal scope of the facts you seek to document. This will assist in defining the appropriate methodology to be pursued.

**Prioritise and plan:** Define your priorities and organise your activities accordingly. Consider where the relevant information is located and how it can best be obtained.

**Coordinate**: Multiple overlapping forms of documentation – such as the repeated questioning of the same individuals by different entities – have the potential to have a detrimental impact on the person and on the usability of their information in future proceedings. Map out similar initiatives by other individuals or organisations operating in the same environment. Build relationships with these other individuals and organisations and coordinate activities with them. Assess what information has already been collected by others and focus your activities. Be prepared to provide interviewees with appropriate identification information so that persons can recall in the future that they spoke with your organisation.

**Logistics**: Ensure you have the necessary equipment, including means of secure communications; make travel and accommodation arrangements, considering the risk environment in which you will be operating and the level of vulnerability of the persons you will be engaging with. Establish a procedure and prepare the technical aspects of the later storage and safeguarding of the information to be collected[1].

## Resources

Ensure that the team is sufficiently diverse (consider gender, nationality, ethnicity, culture and religion, for example) and that the persons involved in collecting information have the necessary skills, competences and training; where relevant, involve a psychologist, an expert in sexual and gender-based crimes and a child specialist.

Conduct a vetting process for all team members, including intermediaries and interpreters. Pay particular attention to any factors that may have an impact on their objectivity or impartiality, or may present risks regarding their security or well-being or that of persons they interact with.

When using intermediaries or interpreters, ensure that they are well briefed on their roles and responsibilities, the security procedures, the confidentiality of the documentation process and the potential disclosure in judicial proceedings of their involvement in the documentation effort[1].

Where relevant, ensure the availability of medical and psychological resources and facilities to carry out required medical and psychosocial assessments. A medical assessment may be necessary, for example, if the witness has recently suffered a physical injury. A psychosocial screening will be required if the witness is in a vulnerable condition or traumatised. Prior planning for the same is essential since such services may not be available on short notice in austere environments.

## Security

Civil society organisations often conduct their work in highly challenging environments, conducting important work as a rapid response to potential atrocities. Reflecting this, while acknowledging that in most cases they operate with a certain level of risk, civil society organisations should exercise due diligence to prevent their activities from putting their own staff, persons providing information, interpreters and intermediaries, affected communities or any other individuals at an unacceptable risk. Consideration should also be given to the risks to the confidentiality of the information and the documentation process. Conduct risk assessments before initiating the documentation process and on an ongoing basis, focusing in particular on:

[1] See Section 12

- **Threats**: Identify threat actors and their capability to cause harm to those involved in the documentation process and the activities themselves. In this context, consider state agents, local militia, foreign forces, and any other persons or groups of individuals.
- **Risks**: When identifying the possible risks of harm consider, among other aspects, retaliation, intimidation, threats, punishments, pressure, bribery, attempts to secure financial gains, re-traumatisation, potential rejection by family/community, job security, financial risks and loss of livelihood.
- **Preventative mitigating measures**: Be aware that the best way to manage risks is to avoid them by following best practices before, during and after the documentation process. For that purpose, ensure the confidentiality of the process and the information, and minimise the disclosure of activities and of those involved. Consider the use of secure communication tools and encrypted storage of information; safe and secure locations for meetings; credible cover stories for participants; code names/numbers for sources of information; and briefing all involved on the importance of keeping their interactions confidential.


© Shutterstock

- **Reactive mitigating measures**: If required, consider discussing with individuals measures that can be put in place to mitigate risks if they arise, such as moving to a safe haven near the person's residence; identifying possible safe routes outside the risk area; assisting the person in moving out of the risk area; determining how to communicate and behave in the circumstances; and determining whether third parties can locally provide support or protection in case of need.
- **Acceptable risk level**: After applying risk avoidance and available risk-mitigation measures, assess the residual risk to yourself, your organisation, information providers or any other person with whom you are interacting. Make your own determination on whether the residual risk is at an acceptable level. Provide information and discuss possibilities, though it should be up to the individual, after being briefed on the risks involved, to make an informed decision on whether to participate in the activity. Record the person's informed consent before proceeding with the activity. Do not coerce someone into activities that entail a risk they are not willing to take, neither impose any risk-mitigation measures on persons cooperating with the documentation process or with whom you are interacting.

Where risks cannot be brought to an acceptable level and remain too high, the documenting activity should not take place. Instead, collect as much information as possible under an acceptable level of risk and be prepared to pass on such information to the competent national or international investigative authorities at the earliest opportunity.

## Confidentiality

Implement measures to protect the information collected and its source, such as codes to anonymise sources, encrypted devices and/or secure communications. Information on documentation activities should be shared on a need-to-know basis.

Explain to the sources of information confidentiality procedures and the importance of keeping their participation in the documentation process confidential.

Ensure that all team members, intermediaries and interpreters are trained in and comply with confidentiality requirements and information-protection protocols.

When there is a need to publicise or share information, seek informed consent as required, conduct an assessment on what can be publicised or shared safely, and what needs to remain confidential.

## Vicarious trauma[1]

Be mindful that anyone exposed to violence, suffering and trauma inflicted on others may themselves experience trauma. Research and be aware of the signs and symptoms of vicarious trauma in yourself and in your colleagues. Define coping measures within your team, and identify services and professionals who can provide support when necessary[2].

[1] Also called 'secondary traumatisation', 'secondary victimisation' or 'compassion fatigue'.

[2] For further details on how to avoid, detect and manage vicarious trauma, see United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh – Trauma-Informed Investigations Field Guide', 2021 ("UNITAD Trauma-Informed Investigations Filed Guide"), Part 7.

# 4. VULNERABLE PERSONS[1]

**As a general principle, civil society organisations should keep their engagement with vulnerable persons for the purposes of documenting international crimes and facilitating criminal accountability mechanisms to the minimum as required to accomplish their mandates.**

This is particularly important when the person is traumatised, a victim of sexual and gender-based crimes ('SGBC') or a child, or in situations where the competent investigative authorities, such as domestic authorities or the Office of the Prosecutor, are already actively investigating.

Any documentation activity involving vulnerable persons, including but not limited to taking a person's account, should be guided by the below principles and best practices.

Engaging to collect information from vulnerable persons should only take place when the information is strictly required, clearly brings added value and cannot be obtained through other sources. When such engagement is deemed necessary, civil society organisations should still aim at keeping it to the minimum required to achieve their purposes, and put in place all the required precautions. That includes using staff who are trained and experienced in dealing with vulnerable persons and involving healthcare professionals, such as clinical psychologists, to ensure their well-being and prevent re-traumatisation[2].

## General considerations

Vulnerability depends on many factors and needs to be ascertained individually. Vulnerable persons can include:

- children (under 18 years of age);
- the elderly;
- victims of sexual and gender-based crimes, torture or other violent crimes;
- persons with disabilities or showing signs of psychological trauma; and
- individuals in detention.

This is not an exhaustive list and other individuals may also experience multiple and intersecting forms of vulnerabilities, conditioned by their socio-economic and cultural contexts, as well as their personal experiences.


© Shutterstock

[1] See also ICC – Victims and Witnesses Unit 'Vulnerability Protocols', submitted in several ICC proceedings: https://www.icc-cpi.int/about/witnesses.

[2] For further details of the relevant precautions to be put in place, see UNITAD Trauma-Informed Investigations Filed Guide, Part 3.

Any engagement with vulnerable persons should be guided by the 'do-no-harm' and 'informed consent' principles.[1] Civil society organisations should adopt a victim- or survivor-centred approach. This means that documenting activities involving vulnerable persons should only take place when it is in their best interest and when they are capable of fully understanding the implications of and consenting to their engagement. In addition, the risks to future criminal accountability efforts that such engagement might pose should also be carefully considered and minimised.

Vulnerable persons face a higher risk of suffering psychological harm when participating in the documentation process (risk of re-traumatisation), may experience difficulties that affect their memory or may be more susceptible to being influenced by those involved in the documentation process. All those factors justify keeping any engagement with them to a minimum and taking all necessary precautions to prevent such risks from occurring.

Vulnerability should be assessed on a case-by-case basis, by conducting a vulnerability assessment and consulting with qualified professionals as required. The goal of the vulnerability assessment is to evaluate whether the person is capable of providing informed consent; the documenting activity can take place without harming the person involved; and to identify the necessary support and protective measures.

A **vulnerability assessment** should:

- Enquire about and evaluate the general physical and mental health of the person and other vulnerability factors (e.g. age, socio-economic and cultural context, discrimination and social-exclusion);
- Consider indicators of potential exposure to trauma;
- Evaluate the nature of the planned documenting activity and whether it can be demanding or invasive to the person;
- Identify measures that can minimise the potential harm, such as adjusting the activity to be as minimally intrusive or harmful as possible; define the support that may be required during the activity (e.g. presence of a support person or psychologist);
- Assess the capability to implement the support/protection measures required to address the person's psychological or physical needs; and
- Consider all of the above and assess whether the person appears capable of providing informed consent and participating in the documenting activity, with the required support being provided, without further harm.

The vulnerability assessment can be conducted by team members with relevant training and experience in engaging with vulnerable individuals and communities. For persons who present signs of trauma[2] and children, a psychosocial assessment should be conducted with the support of a clinical psychologist. Any recommendations made by health professionals must be followed.

**If the vulnerability or psychosocial assessment leads to the conclusion that the planned activity will cause further harm to the person or that support assessed as being required is not available, then the documentation activity should not take place or should be postponed.**

## Trauma[3]

Victims of international crimes have generally been exposed to atrocities and systematic violence which may result in trauma, although not necessarily so. Trauma is an emotional reaction caused by events that may impair the person's ability to function and impact on the person's ability to recall and provide an account of the traumatic experience.

The impact and consequences of trauma vary from individual to individual, but they generally have long-term psychological, medical and social repercussions, which increase the person's vulnerability and the risk of re-traumatisation. Factors such as age, past experiences, personality, cultural context, support and social-integration, as well as the frequency, severity and duration of the traumatic events, can all determine how an individual copes and processes trauma. One of the many possible outcomes of trauma is post-traumatic stress disorder (PTSD), a mental health condition associated with a traumatic event or series of events.

Traumatised persons can reliably convey accurate information. However, trauma can affect memory, sometimes severely. Some may experience intrusive memories (i.e. flashbacks), others may be unable to recall or sequence certain events. Such difficulties can lead to inaccuracies, incomplete accounts or to different versions of the same story.

[1] See Section 2.a and b.

[2] See Section 4.b.

[3] For further information on trauma, see UNITAD Trauma-Informed Investigations Filed Guide, Part 2, p. 16.

Trauma can also affect an individual's ability to regulate emotions and feelings. While some may manage to regulate the negative effects of the traumatic experience, others may not, leading to an inability to control their feelings, reactions and behaviours. Emotional dysregulation can be triggered or enhanced when individuals are confronted with trauma-related cues.

Trauma can manifest in several ways depending on the person. The following are some examples of possible signs of trauma:

- stress, anxiety, fear, depression;
- social isolation or exclusion;
- emotional reactivity or flat affect;
- disorientation, inability to pay attention;
- extreme physical reactions, such as shaking or hyperventilation;
- strong or uncontrolled emotional reactions;
- nightmares, flashbacks and intrusive thoughts/memories;
- avoidance of thoughts, memories, activities, locations, people or other circumstances associated with a traumatic event;
- persistent hypervigilance;
- strong physical sensations or sensitivity to stimuli (e.g. unexpected reaction to noises or smells);
- dissociation: personal events can be described as if experienced by a third-party observer; no emotions are exhibited or emotions are incongruent with facts (e.g. laughs while describing traumatic event); displaying of different personality traits;
- medically unexplained psychological or physical complaints; and
- abuse of intoxicating substances or other addictive behaviour.

Trauma (especially resulting from sexual and gender-based crimes) may also have an impact on self-esteem. The person may develop shame or guilt, which can lead to depression, isolation and difficulty trusting people.

The process of recalling traumatic experiences can also cause psychological harm to traumatised persons. Therefore, when there is a need to engage with traumatised persons for documentation purposes, understanding, recognising and being aware of how to deal with trauma is paramount, as it will minimise the risk of re-traumatisation and ensure efficiency in the documentation activities.

## Engaging with vulnerable persons

When planning and preparing documentation activities, and prior to engaging with vulnerable individuals, ensure that you are ready to conduct the necessary vulnerability and psychosocial assessment and support their physical, psychosocial or other specialised needs. Identify safe and suitable operational options to assist and support vulnerable persons for the purposes of the documentation process. The required types of support may be medical (hospitals), psychological (clinical psychologists), legal (advice and representation), protection (shelters and relocation) and informal services (family, community support). Find out if there are adequate support mechanisms in place to which vulnerable persons could be referred. In their absence, consider whether it is necessary to refrain from approaching such persons.

It is essential that any support or assistance offered or facilitated is not provided or perceived as being in exchange for the person's participation in the documentation process. Ensure that the vulnerable person fully understands this.

Be aware of your unconscious bias (positive or negative) in relation to the perceived vulnerabilities. Be empathetic and respectful; do not be condescending or show pity; and do not assume vulnerable victims are less resilient and reliable.

If required to engage with vulnerable persons, ensure that you are well informed about the nature and potential effects of trauma and that you tailor or, if necessary, cease your engagement accordingly.

While engaging with vulnerable persons, regularly monitor signs of trauma and take the appropriate measures such as:

- reassuring the person;
- keeping a calm demeanour and recognising the person's emotional response as normal;
- considering a break or postponing the activity when appropriate;
- pausing the interview to allow the person to consult with the professional expert or their support person; and
- considering shifting to a more neutral topic.

If serious indicators of risks exist (such as suicidal ideation or desire to harm oneself), immediately consult a healthcare professional.

Once the engagement is finalised, consider the need for follow-up and even, where possible, a referral for additional support to the pre-identified services.

# 5. TAKING A PERSON'S ACCOUNT[1]

## Five guiding principles

**1. Ideally, a person should be interviewed only once with the level of detail required for judicial proceedings. Such interviews should be conducted by the competent investigative authorities.**

Even if well-trained and experienced in conducting interviews, civil society organisations should anticipate that a comprehensive formal interview will nevertheless be required at a later stage and hence avoid carrying out such interviews.

**2. To support criminal accountability efforts, there is no need for civil society organisations to take detailed accounts from persons who may have information relevant to potential investigations and prosecutions.**

This is of particular relevance in relation to vulnerable persons and where the competent investigative authorities, such as domestic authorities or the Office of the Prosecutor of the ICC, are already actively investigating.

Civil society organisations can primarily and very effectively support accountability efforts by identifying and locating victims and potential witnesses, mapping victimisation and alleged crimes, as well as escape routes taken and places where victims and potential witnesses received support or were relocated to. This information should then be preserved with a view to passing it on to the competent investigative authorities at the earliest opportunity to facilitate a future interview.

**3. If and when civil society organisations determine that it is necessary to take a person's account in pursuit of their mandates, but still consider sharing the relevant information with investigative authorities in support of criminal accountability efforts, they should seek to limit themselves to eliciting a first general account[2].**

This means eliciting an account from a person who has not yet been questioned by others (first account) and keeping the information solicited to the minimum necessary to accomplish the purposes of their own mandate, while avoiding a comprehensive and detailed description of the narrated events (general account).

**4. Questioning a person, even if solely for the limited purpose of obtaining a first general account, already carries risks to the integrity of the person's account, particularly if inappropriate questioning techniques are used.**

To avoid inconsistencies with subsequent comprehensive statements, civil society organisations should endeavour to follow good practices, as detailed below, and limit the questioning to the minimum necessary to accomplish their own documentation purposes.

**5. Civil society organisations should refrain from taking an account from vulnerable persons, in particular from traumatised persons and children.**

Civil society organisations should seek instead to focus on efforts to identify and locate victims and potential witnesses and collect the relevant information on such persons, including on their vulnerabilities. This information should then be passed to the competent investigative authorities at the earliest opportunity to facilitate a future interview.

If and when civil society organisations determine that it is necessary to take a first general account in pursuit of their mandates, they should elicit the minimum information required to achieve their documentation objectives, while respecting the do-no-harm principle and ensuring due diligence in applying the recommended best practices.

[1] See also: Mendez Principles – 'New Principles on Effective Interviewing for Investigations and Information Gathering', 2021; Global Rights Compliance LLP - 'Basic Investigative Standards For International Crimes', 2019; Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.4.2, p. 99.

[2] Those representing or providing legal services to victims, other persons or entities in proceedings might be required to obtain a detailed account of events from the persons they represent (as well as from other persons of interest to the proceedings) to competently provide their legal services. However, the present document continues to be relevant in this context, in that it highlights the risks of taking multiple detailed accounts from a person, in particular from those most vulnerable.

## General considerations for taking a person's account

**Individual questioning:** Question each person separately and individually and keep the number of people in the room to a minimum. If there is a need for the presence of persons others than the person(s) doing the questioning, the person being questioned and the interpreter (e.g. a support person, lawyer or legal guardian), then inform those persons in advance that they are not to influence the account of the person being questioned in any way and should not speak during the person's questioning.

Instruct the persons to be questioned that they **should not discuss their questioning or their recall of events with others**, in particular with other persons who have experienced or witnessed the same events, in order to prevent the contamination of the information to be provided. Refrain from 'practice runs' or coaching the persons being questioned.

**Never pay or offer any form of remuneration or any other advantage to a person in return for obtaining an account**. This is not to be confused with the justifiable payment of expenses incurred to organise a meeting with the person (e.g. transport, food, accommodation, and support and security measures).

**Re-questioning:** Avoid seeking an additional account from a person who has already been questioned on the same topic, either by the same organisation or by another organisation, or by the competent investigative authorities. Multiple accounts can – and frequently do – lead to re-traumatisation; inconsistencies in the accounts; weariness and unwillingness to cooperate with official investigations; and increased exposure to risks.

**Continuous contact:** try to maintain as much regular contact as possible with the persons who have provided an account. That will allow you to stay informed of their whereabouts and well-being, and manage these persons' expectations. Otherwise, when those persons are sought (sometimes years later), their contact details may have become obsolete, they may be unreachable or they may have become disillusioned due to the lack of contact and refuse to cooperate.

Therefore, prior to taking an account, enquire if the person has already been questioned by others on the same facts. If this is the case, refrain from questioning them a second time on those same facts.

**Demeanour:** Always remain professional in your interactions with the person being questioned. Be calm, polite, respectful and patient; build trust and respect privacy; pay attention, exercise active listening and respond to the person's needs and concerns; ensure a non-judgemental attitude; be aware of your own demeanour (including body language, pitch and tone); show empathy (not pity); maintain culturally appropriate eye contact; never assume feelings, thoughts or impact of trauma on the person; pay attention to signs of stress, fatigue and trauma; and ensure regular breaks, even if the person does not ask for them.

Use regular breaks to evaluate and discuss with your team the person's demeanour, signs of trauma and distress, and the dynamics of the questioning process, so you can adjust the approach if and when necessary. Throughout the account, assess if and how the questioning can progress.

## Planning and preparation

Good planning and preparation are paramount to ensure the quality of the information provided and safeguard the best interests of the persons to be questioned. For these purposes, consider the following:

- Obtain as much background information as possible on the person being questioned (personal context, affiliations and needs). As required, make arrangements for the care of any children or dependent persons who are under the responsibility of the person.
- Enquire whether the person is represented by a legal counsel. If so, discuss engaging with the counsel, request contact details and, after obtaining the person's consent, inform them that you intend to question the person.
- Conduct a risk assessment prior to initiating contact and review it before eliciting any information.
- Plan your questioning in advance by defining the objectives and identifying the topics you intend to cover.

**Team composition:** Assign trained and experienced interviewers to take a person's account. Where possible, while enabling an environment where the person feels safe and able to express their preference, ask the person if they have any preference regarding the gender, nationality, ethnicity and/or other characteristics of those participating in the process of taking their account.

**Interpretation**: Good interpretation is key. Carefully choose the interpreter, considering, in addition to the necessary linguistic skills, any preferences or concerns expressed by the person. Consider the gender and origin of the interpreter. Some persons may not be comfortable discussing sensitive issues with someone of the opposite sex or with someone from their home town. Vet all interpreters (on relevant affiliations, cultural sensitivities, potential biases or exposure to similar facts and traumas), and brief them on their roles and responsibilities, relevant vocabulary, the profile of the person providing the account and the objectives of the process. In this context, interpretation by family members should be avoided, as much as possible, as it may interfere with the collection of accurate information, may compromise the person's willingness or ability to disclose some events or even interfere with the person's interest to participate in the documenting activity or to engage with other authorities in the future. Train both team members and interpreters on best practices in using interpretation. In particular, interpretation shall be verbatim and reflect, as much as possible, the exact words used by the person, as opposed to paraphrasing or summarising what the person said; those questioning and the person being questioned shall be instructed to speak in small segments and to pause for interpretation; and those questioning shall engage and speak directly with the person being questioned (not through the interpreter). Interpreters should remain professional in their demeanour and not be or appear partial or judgmental.

**Setting the logistics for taking a person's account:**

- **Location:** Choose a location that is quiet, where you can control access and ensure the confidentiality of the questioning process. Create a safe, caring and private environment, where the person feels comfortable to talk about what they have experienced. Identify an area where the person can take breaks and be supported. Where possible, avoid the person's home or place of residence.
- **Assign sufficient time:** consider the timing of the questioning, how the person may need to travel back and forth to the location of questioning, and any security issues or other logistical considerations.
- **Travel planning**: develop a travel plan for the person, bearing mind the safety and well-being of the person. The plan should cover the method of travel, funding for travel, cover story where relevant and accommodation during interview.
- **Equipment**: Make sure you have all that is required to elicit and record the account. Make sure you have refreshments (water in particular) and culturally appropriate food available (e.g. Halal, Kosher or vegetarian food).
- **Culture-specific logistical requirements:** plan for, and take steps to address, any culture-specific logistical requirements. In addition to culturally appropriated food, this may include, for example, allowing for breaks for prayers and providing a prayer mat.

**Remote questioning** is challenging, and can often be a disorienting experience for persons, in particular if not familiar with new technologies. Hence, such interviews should, in principle, only take place when an in-person interview is not possible. Before conducting any questioning remotely (either by phone or using video-conference technology), assess the risks for those involved and for the documentation process. Consider whether the profile of the person is suitable to be questioned without physical presence (vulnerable persons should not as a rule be questioned using such means). Conduct a risk assessment on the potential risk of exposure of the person if questioned remotely. Secure access to adequate equipment, including the availability of a suitable phone or internet connection. Assess the suitability of the venue where the person will be questioned from remotely and, as required, ensure there is local support (which can mean both psychological and technical support)[1].

## Engage and explain

Introduce the team, the organisation and its mandate, and why you are questioning the person.

Take as much time as necessary to explain to the person in detail the purpose and framework of the process. Build a rapport with the person and make sure to address any concerns that they may raise, adapting your language to the person when necessary.

Be patient, and ensure that the person understands all of the above and seek informed consent regarding his or her voluntary participation in the process.

**Obtain biographical details:** Name, date of birth, nationality, ethnicity, marital status, languages, education level, occupation, residence, family

[1] See also: Institute for International Criminal Investigations – 'IICI guidelines on remote interviewing', 2021.

members and contact information (e.g. phone numbers, email addresses and social media accounts). Consider the importance of this data for re-contacting the person providing information in the future and for ongoing and future risk assessments.

**Discuss the importance of confidentiality**, as well as the risks involved and the possible mitigating measures to be put in place. When applicable, update the risk assessment, taking into account the concerns expressed by the person.

**Describe the process:** Types of questions, how interpretation works, breaks, meals and how the account will be recorded.

Highlight the importance of providing an accurate account. Explain that the person is free to answer or not answer any questions; to have information be repeated as needed; that if the person does not remember or know what is being asked, he or she should simply acknowledge that; and that the person has the right to end the interview at any time.

Explain all possible ways that the information to be provided may be used, including that it may be shared with accountability mechanisms and that it may have to be disclosed to the parties in potential future judicial proceedings.

## Account

A first general account captures, in general terms and focusing on essential aspects, the information the person possesses that is relevant for the scope and subject matter of the documentation process. **Keep the questioning to the minimum required level of detail and stop when you have a good general understanding of what the person experienced or witnessed.** Cover relevant topics such as identity, position and role of the person; relevant events and victimisation (including geographic and temporal information of relevant incidents); and identification of the different actors involved, including alleged perpetrators.

Start the questioning with a **free narrative**: Set the general focus of the questioning and initiate it by asking the person to provide a free recall of the relevant events (e.g. 'We are documenting the events that took place in date/location. Please tell us what you know about these events.'). Avoid interrupting the person and do so only if fully necessary to re-orientate the person.


[1] Open-ended questions include the TED questions (Tell, Explain, Describe).

To the extent required to obtain the information necessary and always using appropriate questioning, clarify any topics as necessary, address inconsistencies or contradictions, probe the person on the basis of their knowledge of the facts mentioned; support the person in differentiating what is personal knowledge, what is hearsay and what is common information or beliefs.

**Types of questions:** The aim of the process is to obtain information that captures the person's recollection of events in their own words. The following question types can be used, while recognising and respecting their hierarchical order:

- **Open-ended questions**[1]:they are the safest type of questions as they allow for a full, unrestricted account and produce answers which are less likely to have been influenced by the biases, conscious or unconscious, of the person questioning (e.g. 'Tell me what happened next'; 'Can you describe …?').
- **Probing or focused questions**: also known as the 5-WH questions, these questions give greater control over the direction of the account and can be used to elicit additional information that the person has not yet provided in response to open-ended questions. They may be used to probe, clarify and extend an account that has been elicited through open-ended questions, to cover important information that the person has not already mentioned. Such questions do have the potential to restrict the account, however, so you should return to asking open-ended questions at the earliest opportunity. Examples: 'You mentioned you were outside, WHERE were you exactly?'; 'You mentioned someone called your name, WHO was this person?': 'You mentioned one of the men was using a hand-held radio, WHEN did you first notice this?'; 'You mentioned one of the soldiers verbally threatened you, WHAT did he say?'; 'You mentioned one of your neighbours was shot in the head, HOW do you know?' 'You mentioned that you hid in the bedroom of your house, WHY did you do that?'
- **Closed and forced-choice or 'option-posing' questions**: you may need to ask these types of questions when open and focused questions have failed to elicit any/sufficient additional and relevant information from the person. There is a risk, however, that the person may simply say 'yes' in response to a closed question or select one of the options given, so an answer will always require additional probing. Forced-choice questions, when the options given are defined by the person posing the question, can actually be leading questions. Again, return to asking open-ended questions at the earliest opportunity. Examples: 'You mentioned the church. Did you go in the church?' 'Did he carry the machete in his left or his right hand?'

There are other question types not considered to be appropriate:

- **Multiple questions**: These questions should be avoided as they may create confusion: first, with the person being questioned, who may not know which part of the question to answer; and, second, with those doing the questioning, who may not know which part of the question the answer refers to. It is preferable to break multiple questions into individual ones and ask them separately. For example, 'Where did he come from'; 'What did he look like'; and 'Where did he go?'
- **Leading questions**: Such types of questions should never be asked as they already imply an answer which may adversely influence the person's response by distorting their memory of events, providing them with knowledge or ideas they have not previously revealed themselves, or suggesting there is an answer expected from the person posing the question. The information obtained through these questions can be assessed as less reliable, and as a consequence, they may be given no or less evidentiary weight. Some examples: 'Was the boy carrying a gun or a machete?'; 'Did you hear the commander ordering to attack civilians?'; 'Were the fighters wearing army uniforms?' Instead, use non-leading questions, such as: 'Was the boy carrying anything?'; 'Did you hear the commander speaking?'; 'What was the Commander saying?'; 'What were those fighting wearing?'

Use open-ended questions to the greatest extent possible; restrict the use of the more challenging question types (probing; focused; closed in particular) to extract the level of detail required or to clarify a certain topic under discussion and return to the 'safest' question types at the earliest opportunity (e.g. introducing a new topic). Ask one question at a time, do not ask more questions than necessary and avoid repeating the same question unnecessarily.

Where possible, adopt a chronological questioning structure, but always respect and follow the structure of the free narrative provided,

[1] Open-ended questions include the TED questions (Tell, Explain, Describe).

in particular when the person shows difficulty remembering the sequence of events. Avoid jumping back and forth between topics, as well as between the past and present.

Start with general and neutral topics, moving towards more sensitive ones as the questioning progresses and rapport has been established. If the person shows distress or lack of cooperation, go back to more general or neutral topics and approach sensitive topics again later.

Keep questioning neutral, objective and factual, noting the basis on which the person knows the information provided. Abstain from using legal or formalistic terminology (e.g. 'Was it an attack against civilians'? 'Was it indiscriminate'?) If the person being questioned uses such terminology, try to further clarify what factually happened.

Maintain culturally appropriate behaviour, including suitable eye contact; make responsive statements that acknowledge the person's feelings and concerns; never be judgemental or patronising; be attentive to the person's non-verbal cues, such as tone and volume of voice, eye contact, facial expressions, gestures and body posture.

If the person indicates that he or she has any relevant photos, video, documents or other material evidence of crimes, request that they preserve these and keep them in a safe place in order to hand them over to the competent investigative authorities. Always identify and provide a clear description of any relevant items the person is in possession of in the summary of the account. Each item should be provided with a unique title, so it can be identified by a later reader of the summary. If the person cannot keep the information in a safe place, if it is risky for the person to keep the information, or if the civil society organization is best placed to preserve and keep those items safe, assess the possibility of receiving and preserving them appropriately (for further guidance, see 'Physical items'[1] and 'Storing and safeguarding' such items[2]).

Limit the collection of information on innocent third parties or individuals unrelated to the incident(s), as this might lead to the unwarranted exposure of those persons.

## Closing

Conclude the process of taking the person's account appropriately. Give the person enough time for closure and do not end the process suddenly once the relevant information has been obtained.

End questioning on a neutral topic and acknowledge the person's participation, ensuring that the person is in a positive state of mind. Give the person time to recover and step away from negative thoughts and emotions. As required, apply 'grounding techniques', such as: focus the person's attention on the present moment (e.g. indicate location, date and time; describe the room); suggest to the person that they visualise a safe place or a soothing moment, while taking slow and deep breaths.

Prior to closing, read back to the person the summary of your notes on the account, so that any major errors or misunderstandings can be corrected. Ask also the person if there is any information to add or clarify. Explain what will happen next and address any questions or concerns. Be as truthful as possible and let them know what else they can and cannot expect from you.

Reconfirm informed consent and the voluntariness to participate in the process.

Assess the process with the person. Inquire whether they felt free, safe and comfortable when providing their account. Use the feedback to improve on the following questioning, as necessary. Ask the person to confirm that there has been no threat, promise or inducement that has influenced their account and that they have no complaints about the way they were treated during the process. Such statements can be included in the record of the informed consent.

Reinforce the importance of confidentiality and repeat protection and support measures that can be put in place, as required. Ensure that the person is well informed of the contact details for future communication and any emergency numbers or references provided.

## Evaluation

After completing the process of taking a person's account, take the time to evaluate:

- **The security and well-being of the person**: Review the mental and physical condition of the person and determine whether further assistance (e.g. medical, psychological and legal) may be required. If required, discuss available possibilities with the person and confirm whether they would like to be referred or receive the relevant information

[1] See Section 7.

[2] See Section 12.

and contacts. Review the risk assessment to confirm the potential threats and risks at hand, considering the information provided and, where appropriate, adapt the mitigating measures.

- **The information provided**: Analyse the results of the process and its contribution to the documentation efforts. Conduct a source evaluation analysis, taking note of any facts and information (aside from that communicated by the person) that may be relevant to an assessment of the person's credibility or the reliability of the account provided. Identify possible follow-up activities (leads provided and facts requiring corroboration).
- **The performance of those taking the account**: Make your own self-evaluation and, where possible, discuss the process with your team. Consider the rapport established; the types of questions used; interpretation; and the final outcome. Provide constructive peer feedback.

## Documenting the account

**Civil society organisations taking a person's account should produce a written record of that documentation activity, summarising in it the information obtained as understood by the person(s) taking the account.**

**Civil society organisations should never produce a 'witness statement', i.e. a document signed by the person giving the account. Nor should they make an audio/video recording of the process of obtaining an account.**

When producing a **written record of the person's account**, civil society organisations should seek to:

- place biographical information on the first page. Consider whether to use the person's name or a code for security reasons;
- draft a written summary of the account obtained in what you perceived to be the chronological order of events; draft it in the third person, narrating your understanding of what the person stated (e.g. 'XXX mentioned that…'; 'XXX described the event as…');
- identify and describe in the record any relevant materials the person claims to have in their possession; and include any information regarding their creation, use, provenance, preservation and safe keeping.
- do not record the person's or other participants' opinions, comments, thoughts and analysis and focus only on facts and events. If required, make a separate record for that; and
- ensure the person **does not sign** the written record (as it is not a witness statement);

**Audio/video recording: As a general principle, civil society organisations should not audio/video record the process**. When there is a decision to do so, the following should be considered.

- Obtain informed consent from the person to audio/video record the process (such consent can be captured in the audio/video recording itself).
- Test your equipment to ensure it is functioning well and make sure you have the necessary refills (e.g. extra batteries and memory cards). Be aware of the sound quality for the purpose of future transcripts (e.g. prevent background noise and avoid speaking over each other).
- At the beginning of each recording session, announce the location where the activity is taking place, the local date and time, who is being questioned and who is present in the room, describing their roles. Declare on record any short-term or occasional interruptions.
- If a conversation on the substance of the account takes place while not recording, request the person to summarise such facts on record and make an indication in your written notes.
- Confirm periodically on the record the person's willingness to participate in the process.

## Taking an account from vulnerable persons

**Civil society organisations should generally refrain from taking an account from vulnerable persons. If and when they determine that it is necessary to take a first general account from such persons in pursuance of their mandate, they should elicit the minimum information required to achieve their documentation objectives, while complying with the do-no-harm principle and ensuring due diligence in applying recommended best practices.**

**Civil society organisations should not take an account from traumatised individuals**

**and from children.** Traumatised individuals and children can be particularly vulnerable and should be questioned only once by investigators with specialised training and experience, working for competent investigative authorities. This is to protect the person's well-being and the integrity of their account.

Instead, civil society organisations should collect the relevant information on such persons and pass it to the competent investigative authorities at the earliest opportunity.

If, in what should be exceptional circumstances, civil society organisations assess the need to take a first general account from a traumatised person or a child, they should comply with the do-no-harm principle and be prepared and able to follow recommended best practices.

If the civil society organisation intends to question a person deemed vulnerable for purposes in line with the organisation's mandate, a vulnerability assessment needs to be conducted to evaluate whether the person is fit to be questioned, and what measures can be put in place to mitigate the risk of re-traumatisation[1].

Assess if the vulnerability is likely to affect the individual's ability to freely provide informed consent and to provide an accurate account of the events. Evaluate the impact the process may have on the person (risk of re-traumatisation), even when questioning remains at a general level. When required and possible, in particular when preparing to question persons with signs of trauma and children, secure the assistance of a clinical psychologist or psychiatrist to conduct the vulnerability assessment and provide support as required. **If you are unable to make a vulnerability assessment, do not proceed with the questioning of the person until such an assessment can be made**.

**If the person is assessed as being incapable of providing informed consent or for another reason as being unfit for questioning, do not proceed with taking the person's account.** In such circumstances, collect and record biographical and contact data and all the information available on the person's experience and victimisation. If necessary, and if possible with the person's consent, obtain the relevant information from those who know the person. Record the sources of such information.


[1] For further details regarding the assessment of vulnerable or traumatised persons, see Section 4 and UNITAD Trauma-Informed Investigations Filed Guide, Part 6.

[2] See Section 4 and general considerations in Section 5.a.

The general good practices, described above[2], are of particular relevance when questioning vulnerable persons. They should be tailored to the specific situation and the needs of vulnerable persons. In particular:

- Those taking the account should have relevant experience and training in dealing with vulnerable persons. Include the support of a psychologist or psychiatrist as required.
- Avoid the questioning of traumatised persons, but if they are nevertheless to take place, ensure the support of a trained psychologist or psychiatrist.
- Ensure that interpreters and intermediaries are trained and briefed, so that they understand the potential impact of the process on the vulnerable person.
- Consider having a support person, trusted by the vulnerable person, involved in the process for psychological support (e.g. close relative or guardians for children). When it concerns adults, carefully assess whether the presence of such a support person during questioning, in particular of a relative, may affect the integrity of the account. Discuss with the vulnerable person, when alone, if they feel comfortable speaking in front of the support person about all that they have experienced, as well as the best manner for such support to be provided (e.g. it can be a person who is nearby and available to provide comfort if and when needed).
- To the extent possible, allow vulnerable persons to decide on the meeting location, time, and presence of a support person.
- Keep the questioning at a general level and to the minimum necessary. Do not elicit details about traumatic events, unless really necessary in accordance with the civil society organisation's mandate, to avoid re-traumatisation and reduce the risk of inconsistencies.
- Use questions that are easy for the person to understand. This is particularly important for persons recalling traumatic events. The use of complex language could prevent the person from understanding the questions, which could decrease their confidence.
- Monitor the person's physical and psychological well-being (allow breaks, give space, be kind) and be vigilant for signs of distress and trauma reactions. Use common sense to identify and avoid certain events or details and engage in active listening to detect other potential triggers or unanticipated reactions.
- If the person shows signs of distress, suspend the questioning and keep a calm demeanour. Change the topic, take a break, allow the person to consult their support person and seriously consider closing the process after discussing it with the person.
- Be flexible and ready to adapt your approach, methods and questioning as required. Give the person freedom regarding the sequence in which events are remembered and described.
- After the process, conduct an assessment, ideally with the support of a psychologist, and discuss the need to implement support measures for the person, such as medical care or psychological support.

## Victims of sexual and gender-based crimes (SGBC)[1]

Sexual and gender-based crimes include rape, sexual slavery, enforced prostitution, forced pregnancy, forced marriage, enforced sterilisation, forced nudity and gender persecution, among other acts. Such crimes may be committed against males or females and are not limited to circumstances where physical or sexual violence occurs. They also include crimes directed at a person's gender identity and sexual orientation. Others crimes, such as torture, other inhumane acts, cruel treatment or genocide, may be based on prohibited sexual conduct.

Documenting SGBC presents specific challenges, as these crimes are often under-reported or not reported at all (due to stigma, exclusion from family and/or community, lack of access to justice and support mechanisms, fear of reprisal, psychological impact of past violence and self-blame, e.g.). When documenting SGBC, civil society organisations need to be particularly mindful of the do-no-harm principle and be proactive in their efforts to identify assistance and support services available to which individuals can be referred[2]. Further, civil society organisations may engage with the community and support services (e.g. local leaders, community services, medical facilities and religious entities), in appropriate sensitisation activities to reduce stigma and exclusion and empower victims, to

[1] See also: Global Code of Conduct for Gathering and Using Information about Systematic and Conflict-Related Sexual Violence (the Murad Code), 13 April 2022; United Kingdom Foreign and Commonwealth Office – 'International Protocol on the Documentation and Investigation of Sexual Violence in Conflict', 2nd edition 2017; Women's Initiatives for Gender Justice – 'The Hague Principles on Sexual Violence', 2019; Institute for International Criminal Investigations – 'Guidelines for investigating conflict-related sexual and gender-based violence against men and boys', 2016; World Health Organization – Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies, 2007.

[2] See Section 4.

identify potential victims and witnesses, to ensure the provision of support services and to enable an environment where SGBC victims feel capable and supported to come forward and to provide their account.

SGBC victims are likely to be in a vulnerable condition, or even traumatised, although that is not necessarily the case. If, in accordance with their mandate, civil society organisations a first general account from a victim of SGBC is required, they should initiate the process by conducting a vulnerability assessment to define whether the person is fit to provide such an account and, if so, in what conditions.

When taking a first general account from an SGBC victim the following should be considered, in addition to the general guidelines provided above for vulnerable persons:

- Ensure that those conducting the questioning and the interpreters understand the potential effects of trauma on victims and have specific experience, training and understand best practices in questioning SGBC victims. When required, a psychologist or another mental health specialist should be part of the team to assist the victim.[1]
- Adapt language and references to sex and sexual body parts to the local customs and culture. Note the use by victims of particular vocabulary when making reference to sexual acts or to certain parts of the human body, including non-verbal communication signs. Use body diagrams as necessary to support the victim in identifying certain body parts relevant to the account. Ensure you clarify the meaning of particular vocabulary used to avoid ambiguities.
- During the process, question the victim about any physical items (e.g. clothes) and medical or forensic information that might have been collected at the time of the assault. If they exist, advise the victim on how to preserve them appropriately, given the relevant context, and inform them that the competent investigative authorities may seek permission to collect such items in the future. Whenever possible, refer the victim to a doctor or a forensic professional for them to conduct a medical examination (if possible within 72 hours) and collect any physical items. Ask whether the victim consents to share the information related to the medical or forensic examination with the competent national or international authorities.

**Male SGBC:** In some cases, instances of men and boys as victims of SGBC are reported even less frequently than crimes committed against women. This is because, in some contexts, male SGBC can be taboo, linked to weakness and loss of 'manhood' and the failure to protect the family or community. Such beliefs and fears can make it even more difficult to document these forms of victimisation. Males can also be victims of SGBC by being forced to witness other people being sexually assaulted and/or by beatings administered or aimed at their genitals.

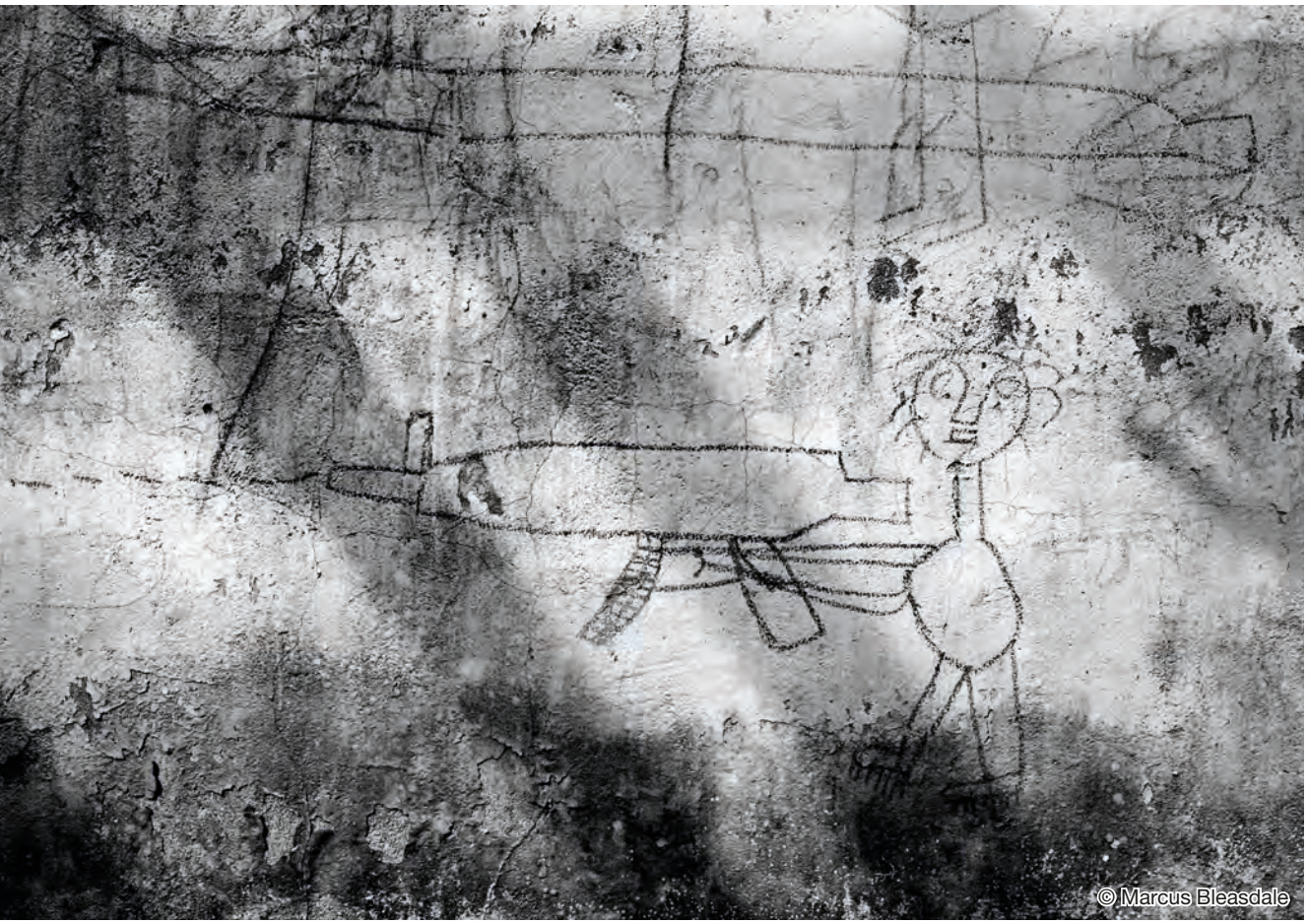
- Be prepared to spend extra time building trust with the identified or potential victims and deal with trauma that might not be immediately visible. Take note of specific signs of potential trauma: closed-off body language; minimal eye contact; avoiding sitting; complaining of lower back pain; expressing strong homophobia; drug/alcohol addiction, HIV; signs of isolation; and expressed disinterest in sex.
- Assistance and support can be inaccessible or inexistent. Prior to the process and as part of the preparation stage, map and vet individuals, expert groups, medical providers, local organisations and community groups of potential assistance to male SGBC victims.
- Address fear of prosecution in contexts where same-sex contacts are criminalised or may give rise to imputed homosexuality.

## Children

**Children (persons under 18 years of age) should be questioned only once by investigators with specialised training and experience working for competent investigative authorities. This is to protect the child's well-being and the integrity of their account. Therefore, as a general rule, civil society organisations should not take accounts from children.**

Instead, it is recommended that civil society organisations collect the child's biographical and contact data and engage with those around the child (parents, caregivers and doctors) to obtain a first general account of what might have happened to the child or what the child might have witnessed. This information should be passed to the competent investigative authorities at the earliest opportunity to facilitate a future interview.

[1] See Section 4.b for guidance on the potential impact of trauma on the person's account.




If, in exceptional circumstances, civil society organisations assess, in accordance with their mandate, that obtaining a first general account from the child is in the child's best interest and is the best course of action (e.g. they are believed to hold unique information that is likely to be unavailable in the future causing their account to be lost), the following should be considered[1].

- When assessing whether to question children, carefully consider their age, development, level of maturity, capabilities and vulnerabilities. In making any such determination, acting in the best interests of the child, informed by the views of the child, their parents or caregivers, is paramount.
- Children are particularly vulnerable and may have suffered special harm due to their exposure to violence. **Children suffering from trauma** may suffer from developmental regression, lack of attention, memory loss or inability for self-regulation. These considerations should be taken into account when deciding whether your engagement is required and is in the best interests of the child.
- Carefully assess the risks, and plan and prepare for taking an account from children. Consider that the questioning needs to be conducted by **persons with recognised expertise in questioning children**.
- Prior to the process, seek to ensure that a **psychologist performs a vulnerability** assessment to assess the risk to the child's well-being, whether the child is capable of being questioned without undue negative psychological impact and which supportive measures need to be put in place.
- **Informed consent**: Engage first with the child's parent or guardian and provide them with a full explanation of the process and potential risks. Prior to initiating the questioning, seek their informed consent for the child to participate in the process. Engage also with the child, providing the necessary explanation in a manner adjusted to the child's age and level of understanding, and enable the child to decide whether they wish to participate in the process. In the absence of parents or guardians, consider other measures to preserve the best interests of the child.

[1] For further details regarding engagement with child victims, see UNITAD Trauma-Informed Investigations Field Guide, Part 4.5. See also the NICHD Protocol in https://nichdprotocol.com.

- Avoid interacting with minors without the **presence of their parent(s) or legal guardian**. Parents have the right to and can be present during the process, in particular for very young children. They should nevertheless be asked not to intervene in the questioning, while supporting the process by monitoring the child's well-being (e.g. pointing out that the child needs a break).
- Adopt **language suitable for the child's** age and development, making sure to create a child-friendly environment. Reassure the child on the process and explain that there are no right or wrong answers and encourage them to answer 'I don't know', if that is the most appropriate response.
- Mainly use open-ended questions and keep the questioning to the necessary minimum (assess whether the child has relevant information and has the potential to be a witness) and be aware that children can be particularly influenced by suggestive questions.
- Regularly monitor the child's well-being and address any distress the child may feel. Offer to take breaks and adapt your techniques for young children (i.e. using a less formal posture).

**Questioning a child victim of SGBC** is a highly complex activity. Children can use a specific kind of language to describe intimate parts and what they endured; some may not be able to understand the harm they have suffered; children may be fearful of denouncing adults. Children victims of SGBC should strictly be questioned only once and by professionals with specialised training and experience in such processes.

If you are aware of the identity of a child victim of SGBC, refrain from questioning them and instead make a record of their personal data and of the information you already possess and refer the victim to the competent investigative authorities.

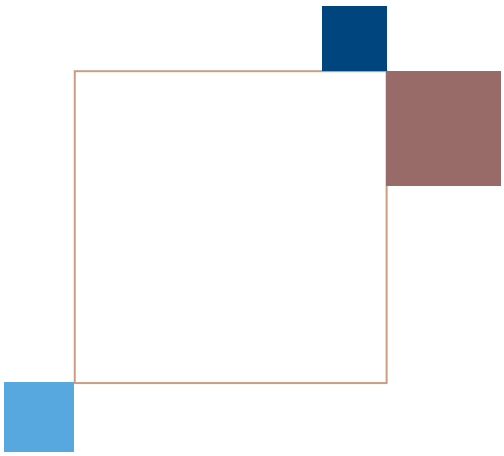
## Persons who may have committed crimes

To preserve the integrity of information and to ensure the safety of members of their team, civil society organisations should seek to ensure that they conduct a specific risk assessment when considering whether to engage with a person they suspect of having committed a crime.

If a meeting or questioning process is to take place, do not actively solicit any information about that person's own involvement in crimes or their role within a group suspected of committing crimes.

If a person spontaneously volunteers information implicating themselves in a crime, reassess the security situation, prior to continuing the discussion.

If and when it is safe to do so (including after concluding the process), record any information received in which a person implicated themselves in a crime. In doing so, reflect the circumstances in which the person volunteered this information, and the precise wording used by that person as much as possible.



# 6. TAKING PHOTOGRAPHS AND VIDEOS[1]

The following is an overview of basic standards that civil society organisations are recommended to follow when taking photographs or videos as part of any activities intended to document crimes and preserve and collect information for accountability purposes.

## Preliminary steps

Remember the **do-no-harm** principle and to first a**ssess security.** If it is unsafe for documenters, their teams, information providers or anyone involved in the documentation process, do not film or photograph.

Be aware of the applicable legal framework regulating the photographing or filming of persons, certain events and locations and, whenever safe and appropriate, first seek the informed consent of those to be photographed or filmed.

**Select the adequate equipment:** Consider resolution capacity, encryption, ability to automatically record relevant metadata, and measures to ensure chain of custody and the integrity of the images. Consider using apps developed for the purpose of documenting human rights abuses and international crimes[2].

**Create a record of the photo/video documentation process:** Describe therein the activity and the methodology used. Identify date(s), location(s), those taking the photos or recording the video and other participants and their role, and the equipment used. Catalogue and clearly identify each photo and video and describe how they are going to be organised and preserved to ensure proper chain of custody (see 'Chain of custody template' in Annex 2). Try to make such records as the images are being obtained, or as soon as possible thereafter.

## Determine what should be filmed or photographed

**Capture the WHAT:** The committing of crime(s), the aftermath and the consequent victimisation (= crime-based information); includes protests, arrests, shootings, bombing, victims, destruction of property; and remnants of weapons and ammunition, for example.

**Capture the WHO:** Who is committing/has committed the crime(s) or any information related to the perpetrator(s) (= linkage information)? This includes soldiers and any armed individuals, military equipment, uniforms, vehicles, licence plates and troop movements). To the extent possible, avoid including bystanders and non-related individuals in the images.

**Capture the HOW:** Any information related to how the crime(s) is/are/were committed. This may include public speeches, relevant meetings, perpetrators giving orders or using communication methods.

## How to take videos and photographs

Make sure to record the day, time and location (WHEN and WHERE) of the images (with GPS coordinates where possible). Configure your device to record as much relevant metadata in relation to the captured images as possible (e.g. location, time, GPS coordinates and device used) for future authentication. Set the calendar/clock to the local time and consider whether it is safe to switch on automatic geolocation and embed information on the author.

Take photographs/videos from different views:

- Start with panoramic images showing the whole scene and general surroundings.
- Move on to mid-range imagery establishing the location and showing the spatial relationships between individuals and/or items and their surroundings (documenting exactly where the item is/was).
- Finalise with close-up images to show key details (e.g. identify people at the scene; licence plates; wounds; letters and marks on items); take shots from different viewpoints of the item in the exact place where it was found; and place a ruler or another measuring tool by the side of the item to indicate the dimensions of what is being photographed/recorded.

[1] See also: Witness, 'Video as Evidence Field Guide', 2016; Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.1.3, p. 75.

[2] eyeWitness, MediCapt, Truepic and KoBo are examples of such apps.

When filming, state for the record the place, date and time of the recording (beginning and ending), as well as the name of the person(s) filming and of any specific persons being filmed. If it is not safe to do so while filming, make sure to capture that information in relation to each recording as soon as viable.

Film a 360° view to provide context and show what is happening behind the scene (or a general view photograph). If possible, film continuously. If not possible, overlap the shots.

## Preserve the videos and photographs

If unable to add the above-mentioned information automatically to the photo or video using technical means, consider creating a summary of the images you have captured (e.g. in a spreadsheet or database). Try to make such a record as soon as possible after the images were obtained; ensure that you are able to identify which photos/videos refer to each summary; record only factual descriptions (what, where, when, how and who), not opinions.

Calculate and record a hash value to the original images to facilitate future verification that the original data has not been modified, tampered with or corrupted in any way. Do not edit or do anything that might alter the original image and, consequently, the hash value (e.g. saving, transferring to others and not using the right tools). If you need to use or edit the captured images, make a working copy while keeping the original intact.

As soon as possible, transfer the images to a storage destination and encrypt all the information (see more below on preservation).

# 7. PHYSICAL ITEMS[1]

Physical items (or artefacts) may be sources of relevant information. They may include, but are not limited to, clothes, weaponry, ammunition, hard copy documents, electronic devices and media carriers. The collection of physical items for use in judicial proceedings should, wherever possible, be conducted in accordance with forensic procedures aimed at ensuring their adequate collection, handling, packaging, transport, storage and preservation, in order to maintain their integrity and evidentiary value.

As a general rule, advise those in possession of any relevant items to preserve and keep them safe in order to hand them over directly to the competent investigative authorities at the first opportunity.

It is recommended that **such items should be collected only in exceptional circumstances**: when official investigators are unavailable to do so; there is a risk that the item or materials will be deteriorated, damaged or lost; the do-no-harm principle can be respected; and the collector is well informed on the procedures to be followed.

© Equipo Argentino de Antropologia Forense, Columbia Law School Human Rights Clinic

[1] Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.3.4, p. 92;

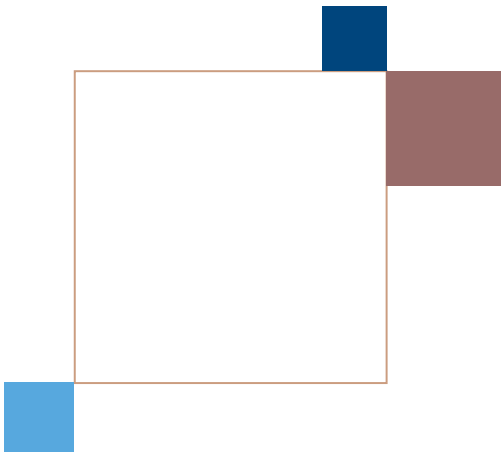
When dealing with physical items, consider the following:

- Be mindful of your own physical safety, your potential liability under applicable law (including in the country in which you are operating) and the potential impact that your activities may have on the forensic value of any physical item that has been collected or preserved.
- Do not collect physical items that might pose a danger to you or others (such as firearms, ammunition, explosives and chemicals) unless you (or someone in your team) has received specialised training and can conduct the activity in compliance with established procedures without endangering anyone.
- Do not use the physical item or try to operate it in any way; that should only be done by a forensic expert.
- As much as possible, apply contamination control measures, such as wearing sterile gloves, when handling the physical items, including documents, to ensure their integrity. Photograph the physical item[1], select the right packaging and label it before placing the physical item inside[2]. Document the collection of the item and its preservation with images (photos/video)[3].

Record the contact details of the provider and seek to obtain consent for the physical item(s) to be handed over to the Office of the Prosecutor of the International Criminal Court, national judicial authorities or other accountability mechanisms. Discuss – and make sure the provider is aware of – how you and others may use those items, the risks involved in being identified as the source of those items, and that he or she takes an informed and voluntary decision when handing over the physical items. Where possible, request the source to sign a dated document recording the informed consent and the handing over of the item.

**Authentication**: Obtain and record additional information about an item (including documents and digital information) to establish its authenticity. To that end, take the following measures:

- Record an account from the provider on the origin of the item, when, where and for what purpose it was produced and obtained (see 'Chain of custody template' – Annex 2), as well as the circumstances in which the provider obtained it and is handing it over.
- If the item originated from a person other than your source, try to identify the original provider or originator of the document and, where possible, locate and record an account from that individual on the item.
- Consider obtaining and recording an account from other individuals who might be able to provide additional information on the authenticity and origin of the item.
- Prior to proceeding with further enquiries, assess the risks involved to you and your team, as well as to the originator or the previous source of the documents. If such risks are not at an acceptable level, do not proceed and instead keep a record of potential sources of authentication that you can then share with accountability mechanisms who may be in a better position to question such individuals.



[1] See Section 11.d.

[2] See Section 12.

[3] See Section 6.

# 8. DOCUMENTS AND DIGITAL INFORMATION[1]

Documents can be digital information or physical items (hard copy documents) and cover a variety of categories, such as official documents (e.g. minutes of official meetings and military documents), financial records (bank statements and transactions), medical records, maps and diaries. Some documents might be protected by state secrets or privacy rights. Therefore, be aware of the applicable legal framework and the potential risks involved in receiving or being in possession of certain documents. Documents containing private or personal data should be kept confidential and preserved in a manner that prevents their contents from being unduly disseminated.

- The same principles described above, including those relating to the collection or preservation of physical items, apply to the collection or preservation of documents and digital information.
- Do not alter the documents received, regardless of whether they are the original versions or copies. Wherever possible, use sterile gloves when handling the documents. Take photographs and, if required and you deem that it will not further damage the document, make photocopies, prior to placing the original document in a suitable package, properly labelled to prevent loss or damage.


[1] See also: Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.1, p. 61; European Union Agency for Cybersecurity – 'Electronic Evidence – A Basic Guide to First Responders', 2015.

## Digital Information

Digital information is data stored or transmitted in digital format (e.g. photos, videos, posts on social media and emails). Digital data is fragile and volatile, as it can be changed, destroyed or altered very easily, either deliberately or through improper initial recovery, preservation, handling or storage. As best practice, electronic devices containing digital data should only be handled by forensic experts to avoid contamination and ensure the integrity of the device and the data therein. Digital information is documentary information, to which technical considerations apply. Therefore, all the above guidance applies with the required adjustments. In addition, apply the following measures:

- Plan for and take steps to minimise alterations of digital information and document steps taken during its initial recovery and preservation.
- If possible, collect the original physical storage media (e.g. laptop, phone and tablet), applying strict contamination control measures for physical items (see above) and keeping the device stored safely for further examination by a forensic expert.
- Note any relevant information (device switched on/off, make and model).
- Where possible, and after obtaining and documenting the informed consent from the owner of the device or of the information:
  - Obtain and record in your notes any available passwords, encryption keys or other authentication data that will allow future access to the digital information.
  - Consider the possibility of the device being connected to a cloud service where data is stored and requested. Where legally possible, obtain and record the access credentials.
  - Where legally appropriate, request and record access to the credentials of any remote platforms that the device is connected to and where relevant data might be stored.
- If the device is switched off, do not switch it on. If it is switched on, and you do not have the required access credential and/or encryption key, take photographs of what is displayed on the screen or monitor, consider isolating the device from any network and take the device as soon as possible, while keeping it switched on, to a competent forensic expert for appropriate instructions regarding seizure and preservation. If possible, seek specific advice about imaging RAM and checking for encryption before powering down the device.
- Collect any peripherals, including cables, adaptors and chargers, cartridges and user manuals.
- Photograph the device together with associated accessories, cables and connections.
- Do not use or try to explore the data within the device (it can lead to alterations of the data, thereby compromising its integrity).
- Label, package and seal the device and each component separately. If a device is too large for a bag, wrap it in paper.

As a last resort, in cases where it is not possible to collect and preserve the device, it is not available at a later stage for forensic examination by the competent investigative authorities, and the data contained in it is important and will be lost if not extracted, secure the assistance of a digital forensics expert to conduct a f**orensic acquisition of the data** (to be saved as a 'Master Copy'). The process should be thoroughly documented by the person conducting the forensic preservation. If necessary, request the forensic expert to create Working Copy from the Master Copy, which can then be used to review the extracted information, while keeping the Master Copy intact.

# 9. ONLINE INVESTIGATIONS[1]

Online investigations refer to the use of the internet to identify and collect relevant information. The following is an overview of basic standards that civil society organisations should seek to follow when conducting online investigations intended to preserve and collect information for accountability purposes.

Consider, at all times, whether you might be in breach of any applicable legislation and also whether you are exposing yourself and others to unacceptable risks.

**Online security:** Conduct a security assessment on the digital landscape before initiating any online activities. Define and implement a digital infrastructure that will adequately safeguard any risks to your organisation, the documentation process, external sources of information and any other relevant third parties. To the extent possible, avoid using personal equipment in online activities and consider using a virtual machine. Ensure training on online enquiries to those who will be assigned to conduct such activities. Assume that your online activities may be monitored by third parties and, as much as possible, aim for them to remain anonymous and non-attributable .

Online information is highly volatile – it can disappear from the internet or be easily modified. Therefore, capture online information in such a way that enables the authenticity and the integrity of the digital item to be established as collected at a certain time from a certain web location. To that end consider the following:

- Once information found online is assessed as relevant, determine the proper method of collection. While for work purposes a simple screenshot or a PDF conversion might suffice, for online content assessed to contain potential probative value, collection should entail the download or recording of the online content and all related information (as indicated below) and the assignment of a hashtag. Such collection can be done manually or with the use of tools specifically developed to collect and preserve online content[2].
- Collect online materials in their native format or as close to their original format as possible.
- For each item of online material collected, ensure to capture at a minimum the following information (or that the tool being used automatically does so):
  - o target web address (URL);
  - o HTLM source code; and
  - o 'screen capture' or 'full page capture' – a screenshot or video of the target web page (depending on the content), with an indication of the date and time of the collector's system.
- Additional information to be captured:
  - o **embedded media files:** If the webpage contains a variety of content, including different videos or images, each relevant item must be collected individually;
  - o **embedded metadata:** If available, common metadata, such as uploader ID, post, upload date and time, hashtag and comments, should also be collected;
  - o **contextual data:** If relevant, related data, such as comments, user information and upload and uploader/user information, should also be collected;
  - o **collection data:** Record all relevant data pertaining to the collection of the online materials, such as name of the collector, IP address and collection start/end time stamps of the device used for the collection[3]; and
  - o Consider capturing network traffic during the preservation (e.g. TCP dump).
- Calculate and record the hash value[4] of each digital item collected and store items collected in a new/clean media device.

[1] See also: Office of the High Commissioner for Human Rights/Human Rights Center UC Berkeley School of Law – 'Berkeley Protocol on digital open source investigations', Advanced version, 2020 [Berkley Protocol].

[2] Many of these tools automatically download the online content, collect the relevant metadata, hashtag the information and create a digital package with all the relevant information.

[3] Ensure that the system clock of the device used for collection is accurate, preferably by synchronising it with a Network Time Protocol server.

[4] There are many hash values and tools to generate them to choose from. The United States National Institute of Standards and Technology is one organisation that provides guidance on the current standards for hashing information. See www.nist.gov.

# 10. PHYSICAL INJURIES[1]

As a general rule, **only a qualified medical practitioner can medically examine a victim**. If such professionals are not available, it is recommended that civil society organisations limit their interactions with victims to only document visible injuries. Instead, they should encourage and support victims to seek professional medical attention and to preserve all records.

Seek informed consent from the victim prior to documenting physical injuries and record the informed consent.

Make clear to the victim that you are not a medical doctor.

Upon receiving informed consent, record visual information of external injuries. Make sure to have an overall description of the location of the injuries and a detailed one; where allowed to record the injury, do a close-up, a mid-range and a general picture of each injury.

Take an account from the victim regarding the causes of those external injuries, the instruments used and the manner in which the injuries were inflicted; take note as well of any long-lasting consequences, such as persisting pain and related symptoms.

Keep a record of every action taken and your own observations about the injuries.

Examination and documentation of injuries to private/intimate parts must only be conducted by a medical doctor or qualified nurse.

Ask the person whether they have visited a doctor or a medical facility in relation to their injuries. If so, collect the identifying information of the medical provider.

If required, consider referring the victim to an identified suitable location for further support or further medical examination.

Remember that medical information and documentation is very sensitive personal data with a high level of privacy attached. Therefore, such data should only be obtained with consent from the owner of the information and should be protected from any unwarranted access.


[1] See also: Office of the High Commissioner for Human Rights – 'Istanbul Protocol: Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment', 2nd edition, 2022. Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.3.1, p. 85.

# 11. CRIME SCENES[1]

**As a general principle, when confronted with a crime scene, civil society organisations should not enter or disturb it in any way. Instead, they should immediately contact the appropriate authorities, while putting in place available measures to prevent others from contaminating the crime scene. This is of particular relevance where the competent investigative authorities, such as domestic authorities or the Office of the Prosecutor, are already actively investigating.**

Civil society organisations should only consider to intervene in exceptional circumstances, namely where:

1) no competent investigative authorities are willing or able to secure the location in a timely manner or, where possible and advisable, they have been notified that such intervention is under consideration and have assented thereto;
2) not examining the location before competent investigative authorities are available is very likely to result in significant degradation of the crime scene, so that crucial information may be lost or suffer irreparable damage;
3) the do-no-harm principle can be respected; and
4) the civil society organisation has recourse to professionals with training and expertise similar to those of national authorities in processing crime scenes and can do so in a manner that will enhance rather than potentially undermine the future use of the information obtained in a criminal investigation/proceeding.

If there is a decision to intervene, consider the following:

- Be mindful of your own physical safety and that of others. Consider your potential liability under applicable law (including in the country in which they are operating), and the potential impact that your activities may have on the forensic value of any information that you collect or preserve.
- **Security**: Conduct a risk assessment and only intervene if the site is safe and free from danger (for you, the team, others present or involved and for the information itself). Consider potential hazards (e.g. fire, mines, bombs and chemical products); the presence of perpetrators; the need for specialised equipment; and possible accidental destruction/damage of relevant objects or sources of information. **Do not proceed if any identified risks are assessed as being at an unacceptable level.**

## Principles of crime scene examination

Maintain **objectivity and impartiality**: Collect both incriminating and exculpatory information.

Respect **privacy and human dignity (= do-no–harm principle)**, including the interests of the impacted community and the surviving victims.

Maintain the **crime scene integrity** by adopting contamination control measures, as described below.

## Secure and preserve the integrity of the crime scene

Identify and prepare all necessary tools and equipment.

Create a team with the necessary skills and competences, as required.

Define and demarcate the site and establish entry and exit points.

Identify all persons who are or might have been at the crime site.

Limit access to the site and maintain a log of all persons entering and leaving the site.

Wherever possible, ensure that those entering the site wear personal protection equipment, including sterilised gloves.

Do not eat, drink, smoke or use facilities on the site.

## Document your examination of the crime scene

Create a record containing all relevant information on both your activities and your findings, including date and time of arrival, location; general

[1] Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.2, p. 79; United Nations Office on Drugs and Crime – 'Crime Scene and Physical Evidence Awareness for Non-Forensic Personnel', 2009.

description of the overall crime scene (to be complemented with sketches, photos and videos); anti-contamination measures in place, including the log of all persons who entered the site (when, how long and why); a detailed record of your methodology and of the information collected at the crime scene; and any accounts taken from those present.

Photographs or videos should be taken prior to any disturbance of the scene[1].

Create all notes and make all observations on the record at the time of the examination and do not alter the record at a later stage. Make sure to keep the record as factual as possible. If you need to record your opinion, assessment or conclusions, identify it as such in the record to differentiate this from the recorded facts.

Remember that such records may be disclosed at a later stage in judicial proceedings, including the identities of those participating in these activities.


[1] On photos and videos, see Section 6.

## Processing the crime scene

Do not touch or collect dangerous items. If an object appears to pose a threat, take images and record findings, but do not collect it.

Evaluate the items found and consider carefully which items can and are to be collected/preserved; in such assessment:

- Consider any detrimental effects the recovery process will have on the item.
- Ensure that the recovery technique neither destroys, nor contributes to the deterioration of the item to be collected, or other items.

Collect items as soon as possible after their discovery has been documented; secure fragile items immediately after photos/video are taken.

Package items appropriately in containers or packages that do not contribute to the decomposition of the contents and can protect them from shocks, humidity and extreme temperatures[1].

Establish a safe, secure area on-site for temporary storage. As soon as possible, move the collected items to a permanent secure location and follow the preservation procedures described below.

Obtain the contact details and consider questioning some of those present at the crime scene to obtain a first general account of what happened and, as required, to obtain additional information on the collected items.

If faced with dead **human bodies**:

- record and document your factual findings, without touching or disturbing the bodies;
- film or photograph the bodies, including visible injuries (e.g. bullets and stab wounds), signs of ligatures, cloths and other personal accessories and details (to support future identification); and the shape(s) and spread(s) of bloodstains;
- if possible, collect information in relation to the identity of the victim(s) (e.g. gender, name and address); and
- follow up with the local community and, where possible, the local authorities in relation to the burial of these bodies and keep a record of where each body was taken and eventually buried.

## Documenting burial sites and mass graves[2]

Exhumations and autopsies should only be conducted by certified practitioners (e.g. forensic pathologists and clinical forensics). Only such professionals are considered experts, can produce forensic reports and will be able to testify in court regarding their findings with the required level of expertise for them to have any evidentiary value.

If such professionals are not available when faced with mass graves, consider the following measures:

- Report any burial sites or mass graves to the relevant authorities, unless those authorities might be involved in the killings and/or might tamper with information.
- Limit your actions to preserve critical information on the burial site.
  - o As a priority, preserve the crime scene by closing or limiting access to the site as much as possible.
  - o If bodies are well buried, do not to touch the graves and keep the integrity of the burial site(s) until professionals can take action.
  - o Take notes and record your findings, including the exact location of the relevant site(s) using GPS coordinates if possible.
  - o Document and record the scene(s) through filming and/or photos.
  - o Build relationships and trust with the local community and sensitise them to the need of securing the site(s). If the existence of the site is unknown, consider the possibility of not disclosing its existence to the community to preserve its integrity and find other ways of monitoring the site's integrity.

[1] See Section 12.

[2] See also: Bournemouth University – 'The Bournemouth Protocol on Mass Grave Protection and Investigation', 2020. Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 3.3.3, p. 88.

# 12. STORING AND SAFEGUARDING[1]

The following is an overview of basic standards that civil society organisations should seek to follow when storing and safeguarding any kind of information that they have collected for accountability purposes.

Preserve the integrity of each item and piece of information collected, from the moment it has been obtained to the moment when it is handed over to the competent investigative authorities. During that period, take the necessary measures to ensure that the item and the information collected are not damaged, lost, altered or tampered with.

Conduct a risk assessment in relation to the best location, methods and processes to preserve and store the information, and consider doing it in other countries as required.

Be mindful of applicable legislation concerning the protection of personal data.

Keep a thorough and unbroken record of the chain of custody for every piece of information collected, describing thoroughly and in detail its whereabouts, and identifying every individual who accessed and handled the information, from the moment it was originally received or created to the moment it is handed over to an investigating authority. When creating a chain of custody log, consider using the 'Chain of custody template' in Annex 2.

Apply proper information management practices, from the moment you create or receive information. Such practices should ideally be set out in your internal standard operating procedures or manuals, as they will be essential to evaluate and determine the authenticity of the information or item and the likelihood of someone having tampered with it.

Create a **log or database of the collected information** in which, for each item collected, the key data identified below is recorded (when not possible, record the reason why and any alternative measures applied):

- date, time and location of collection of the information;
- a brief description of the item (e.g. x number of pages of medical records; x pen drives and x laptops containing data; x number of photos/videos);
- name of the creator or collector, as well as the name of the provider of the information (if applicable);
- known information on who had access to the information or item, from when it was generated until it came into your possession, as well as the source's motivation for sharing the piece of information;
- the exact location of where the item has been stored at each moment of time, from the moment it has been received to the moment it is handed over to the competent investigating authorities, including the name of the person(s) who is(are) responsible for preserving and controlling access to the item;
- a detailed record of everyone accessing the information, mentioning in relation to each item accessed: date/time (start and end of access); where the item was accessed (ideally, it should stay where it is stored and be consulted there) and for what purpose (reasons for access). Also include information in relation to the sealing and re-sealing of packages; and
- consider creating a separate record for highly sensitive information or use codes to protect the names of the external sources of your information.

**Packaging:** Every item collected should be properly packaged to ensure its safe keeping and prevent its deterioration. The appropriate packaging will depend on the nature and the size of the information collected. Consider the following:

- Prepare the right equipment in advance.
- Package items that contain biological material (e.g. blood and body fluids) or any residual moisture in paper containers (not plastic).
- Dry items before packaging. If that is not possible in situ, transport the item in a paper bag until it can be dried in a safer location and then be properly packaged.
- Any packaging must be clean and unused.
- Use as many layers as required to prevent odours or to protect the items from excessive movement, heat, shock and humidity during transportation and storage.
- If an item is too large to be packaged, wrap it in paper. If that is not possible, attach the label to the item and store it appropriately.

[1] Public International Law & Policy Group – 'Handbook on civil society documentation of serious human rights violations', 2016, Section 4, p. 116.

- Be ready for the need to improvise packaging; apply common sense and use the materials you have at hand, as long as they are clean or unused (e.g. a piece of paper can be used as an envelope and a plastic bag can be used as a seal bag).

**Labelling:** Label packed items for easy identification without having to open the package. Develop a label that contains basic relevant information on the item: general item description; date, time, location of the collection; name of collector and name of external provider, if applicable and safe. For security reasons, consider assigning the package a unique identification number that connects it to the relevant data recorded in your log/database of collected information. Label the packaging before placing the items in it. Only label or mark items directly in exceptional circumstances (e.g. when too big for packaging). Place a warning label on packages containing potentially hazardous materials (i.e. biological or sharp items).

**Sealing:** To demonstrate that the packaging has not been altered or tampered with, use tamper-evident seals (i.e. strong adhesion tape), close the package with it (using a single strip of tape), and sign and date the seal. Do not use staples, office tape or adhesive envelopes as they can easily be opened and rapidly lose adhesion. As a general rule, do not re-open a sealed bag. If, in exceptional circumstances, a sealed package needs to be opened, cut the package open in a single line at a distance below the original seal and re-seal it. Ensure the date, location, those involved and the reasons for unsealing are thoroughly documented in the chain of custody log.

**Cataloguing:** When dealing with a large amount of collected information, ensure that all information collected or received is easily retrievable. Organise it thoroughly to ensure a good overview of what was collected and to enable each item to be easily found and retrieved. Create a document or database recording basic information on all materials collected.

**Storage:** Depending on your resources (i.e. physical space and available material), choose adequate physical and digital storage systems. For security reasons, highly sensitive information should be stored separately, using enhanced security measures. Consider the following guidance in relation to storage.

- Catalogue all items with a numbering system. Make copies of important information and keep copies separately in a safe place.
- Store highly sensitive information separately, while ensuring the confidentiality of all items. Depending on the storage system, lock or encrypt confidential information and try as much as possible not to draw attention to it.
- Encode information as much as possible using codes or pseudonyms (e.g. using code names for external sources or information and keeping the key to those codes safely and separately).
- Limit access to information and base it on the 'need-to-know principle': the fewer people who have access to the information, the better it is preserved. Define clear instructions to control access to the information (see above).
- Develop an emergency security plan in case any information is put at risk. Do not destroy information unless there is a tangible risk.
- **Physical storage:**
  - Keep information in a locked storage facility (i.e. safe or cabinet), safe from fire, water, extreme temperatures and insects.
  - Keep items part of a set stored together (i.e. documents collected together).
- **Digital storage:**
  - Make sure that your operating system and software are up to date.
  - Use an encrypted storage device that is easily transportable and can be easily hidden (e.g. USB, flash drive, SD cards or external hard drive).
  - When/while information is stored on devices with an internet connection, which should be avoided, equip them with appropriate anti-virus, anti-spyware and firewall software.
  - Always store sensitive information on devices that are encrypted[1] and not connected to the internet, and access them from non-connected devices.
  - Store the digital information in folders, logically organised to be easily retrievable.
  - To prevent loss, ensure information is regularly backed up. Verify that your backup solution works and that you are able to restore all your data in case of data loss.
  - Do not connect the Master Copy of a forensic extraction to another device.
  - If using cloud storage services to store your information, enable multi-factor authentication on your account and select providers that offer full data encryption; use strong different passwords to protect the data and if possible, do not use public Wi-Fi to access it or make sure to have your VPN enabled.

[1] You can find free encryption tools on the internet, such as: AxCrypt, BitLocker, GNU Privacy Guard.

# 13. ANALYSIS OF COLLECTED INFORMATION

The competent investigative authorities will always conduct their own independent analysis of the information they obtain, including material received from civil society organisations. This should not prevent civil society organisations from conducting their own analysis as required according to their mandate, objectives and legal framework. In fact, such analysis can be of great use for accountability mechanisms.

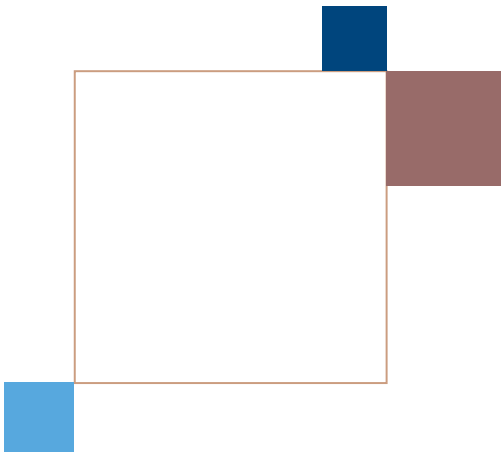
Information analysis by civil society organisations accompanying the collection of information is particularly helpful if it involves large data sets – such as collections of videos, radio communications, electronic data, social media information and financial information – or if the underlying information requires technical or scientific analysis.

When conducting analytical work, civil society organisations are recommended to carry out such activities in line with the following principles.

- Conduct analysis in a manner that does not affect the integrity and chain of custody of the collected materials it uses for its findings.
- Record your analysis separately from the records created to capture the factual information collected.
- Include clear references to the information or materials used, as well as the employed methodology, so third parties are able to reconstruct and review the analytical thinking.

When collecting information that may be of relevance for accountability purposes, the following analysis may particularly help to optimise the usefulness of that information for the competent investigative, prosecutorial and judicial authorities:

- **Source evaluation:** Make your assessment of the credibility of the source of the information and the reliability of the information itself. Record not only your conclusions, but also the information, facts and reasons underpinning it. Identify and address any potential inconsistencies and weaknesses of the information.
- **Contextualisation of the information:** Connect, link and compare the information collected. Look for similarities and/or inconsistencies, identify links (e.g. items from the same source or location and individuals, locations, events referenced in different items). Identify when certain information is corroborated by other information.
- **Strengthening of the information:** Identify leads that will allow for the collection of additional information to complement and/or corroborate the information already obtained.



# ANNEX 1:
# INFORMED CONSENT TEMPLATE

*Your informed consent is required to both collect and use information you can provide. By giving your informed consent, you recognise that you have been informed and that you understand the nature and the scope of the documentation activity, accept to participate in it and accept that the information you provide can be shared with the competent national and international investigative authorities. By signing this document, you are providing your informed consent.*

I hereby acknowledge and confirm that:

- This is a voluntary process and I have provided information, documentation or physical items freely, without any form of coercion, threat or duress.
- I was informed that the information, documentation or physical items I have provided might be used in criminal investigations and/or prosecutions and be shared with the competent national and/or international investigative authorities, including the Office of the Prosecutor of the ICC.
- I am aware that my identity, as well as any information I have provided, might be disclosed to the parties in future proceedings.
- I understand the nature and the purpose of the documentation activity, the potential use of the information I have provided, as well as all the potential risks associated with my participation in this activity.

I hereby consent to:

☐ [Indicate/describe consented activity (e.g. give an account; hand over documentation or other items; being photographed and document physical injuries].

☐ Sharing the information, documentation or physical items that I have provided with the Office of the Prosecutor of the ICC and their use in criminal investigations and/or prosecutions.

☐ Sharing the information, documentation or physical items that I have provided with national authorities or other international judicial mechanisms and their use in criminal investigations and/or prosecutions.

☐ Any limitations: _____

_____

**Name:** _____

**Signed:**_____

**Dated:** _____

# ANNEX 2:
# CHAIN OF CUSTODY TEMPLATE

*To be completed by the information custodian*

Date of collection: _____

Location of collection: _____

Received from: _____
*(If applicable)*

Support: _____
*(Describe the type of information)*

Received by: _____

Organisation: _____
*(If applicable)*

Circumstances of Collection _____

_____

_____

Description of the piece of information collected *(including condition, value and reason(s) for collection):*

_____

_____

_____

_____

_____

_____

Name/signature (Custodian): _____

Name/signature (Depositary): _____

| Date and time: | Released by: *(Name, Signature)* | Received by: *(Name, Signature)* | Purpose of release: |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

# ANNEX 3:
# CHECKLIST FOR CIVIL SOCIETY ORGANISATIONS

This checklist is annexed to the Guidelines for civil society organisations engaged in the documentation of international crimes and international human rights violations for accountability purposes. It sets out core principles and critical steps in undertaking such activities.

This checklist is not intended to provide an exhaustive overview of international standards and best practices detailed in the Guidelines, but it is intended to be used as an aide memoire in support of the Guidelines.

Civil society organisations are encouraged to consult the Guidelines prior to starting any documentation activities.

| 1. GENERAL PRINCIPLES | |
|---|---|
| **Do no harm** | ✓ Act in the best interest of persons providing information, intermediaries, local communities and any other person involved in the documentation process, including yourself.<br>✓ Assess and mitigate any potential negative impact on future evidence collection or accountability efforts by official national/international authorities.<br>✓ Prioritise security, physical/psychological well-being and privacy of the person<br>✘ Do not undertake activities that expose any person involved in the documentation process to any risk that might cause harm or compromise future evidence. |
| **Informed consent** | ✓ Obtain informed consent of the person or entity with which you engage prior to any information-gathering exercise.<br>✓ Consent must be:<br>➤ **informed:** give a full explanation of the nature and purpose of the activity, the procedure that will be followed, the potential use of the obtained information and the foreseeable consequences of sharing information, including potential security risks;<br>➤ **contemporaneous:** ensure the person understands that they can withdraw their consent to cooperate in the activity at any time and that consent to share the information provided can be withdrawn until such information is shared with national authorities, ICC or other international accountability mechanisms. Renew the informed consent on an ongoing basis as activity progresses;<br>➤ **voluntary**: respect free will and ensure the person gives their consent voluntarily. Be mindful of social contexts that might inhibit the person's ability to freely consent to the activity; and<br>➤ **explicit:** produce a record of the provision of informed consent in a signed document.<br>*See Informed consent template – Annex 1 to the Guidelines.*<br>✓ Ask the persons for their informed **consent to share the information obtained** with any competent national or international investigative authorities and explain the parameters of confidentiality, subject to applicable rules.<br>✘ Do not give unrealistic guarantees or make promises about the future use of the information.<br>✓ Once you have obtained the informed consent of the person for the information to be shared, securely preserve the information with the view to provide it to competent national or international investigative authorities at the earliest opportunity.<br>✓ If sharing information with multiple jurisdictions, inform each jurisdiction to facilitate coordination. |

| | |
|---|---|
| **Objectivity, impartiality and independence** | ✓ Carry out your activities in an objective, impartial and independent manner, consistent with the collective aim of discovering the truth.<br>✘ Do not make assumptions; do not influence information providers; and do not take a specific side during your documentation process.<br>✓ Document incriminating and exonerating information equally.<br>✓ Act free from any interference or influence by any authority, person or organisation. |
| **Accountability and legality** | ✓ Be mindful of potential liability under applicable laws, especially in the country in which you are working.<br>✓ Remember that you are not acting under the direction of or on behalf of official accountability mechanisms.<br>✓ Maintain a detailed record of your methods and procedures to preserve and collect information. |
| **Professionalism and respect** | ✓ Always act with professionalism, integrity, respect and empathy, and remain mindful of cultural sensitivities and vulnerabilities at all times.<br>✘ Never pay or offer any form of remuneration in exchange for information. |

| 2. PREPARATION | |
|---|---|
| **Early preparation** | ✓ **Research your operational environment**, paying attention to type(s) of alleged criminality; parties involved and potential perpetrators; vulnerability of the population; general socio-cultural, political and religious context; and applicable legislation.<br>✓ **Define your mandate, objectives and focus**: determine the geographical/temporal scope of the facts you seek to document; prioritise and plan your activities accordingly.<br>✓ **Coordinate**: map out and coordinate with similar initiatives by other individuals or organisations operating in the same environment. Assess what information has already been collected by others and focus your activities.<br>✓ **Logistics:** ensure adequate equipment, travel and accommodation arrangements, and secure communications, e.g.. |
| **Resources** | ✓ Carefully select and prepare your team (consider gender, nationality, ethnicity, culture and religion, e.g.).<br>➤ Ensure your team has the relevant skills, competences and training.<br>➤ Where relevant, involve a psychologist, a sexual and gender-based crimes expert and a child specialist.<br>➤ Conduct a vetting process for all team members.<br>➤ Brief intermediaries and interpreters on their role and responsibilities, the importance of security and confidentiality, and potential disclosure in judicial proceedings of their involvement. |

| | |
|---|---|
| **Security** | ✓ Ensure that your activities do not put your own staff, persons providing information, interpreters and intermediaries, affected communities or any other individuals at risk.<br>✓ **Threats**: identify threat actors and their capability to cause harm to those involved in the documentation process.<br>✓ **Risks**: consider, inter alia, retaliation, intimidation, pressure, bribery, re-traumatisation, rejection by family/community and job security/ financial risks.<br>✓ **Conduct risk assessments** and **apply mitigating measures** (preventive and reactive) to lower risk levels.<br>✘ **Do not engage in** documentation activities where risks cannot be brought to an acceptable level. |
| **Confidentiality** | ✘ Do not discuss the documentation process with third parties.<br>✓ Keep the information collected and sources strictly confidential.<br>✓ Implement confidentiality mechanisms such as **codes to anonymise sources, encrypted devices or secure communications**. |
| **Vicarious trauma** | ✓ Be aware that you may suffer trauma as a result of the continued exposure to violence, suffering and trauma inflected on others.<br>✓ Research and be aware of the signs and symptoms of vicarious trauma in yourself and in your colleagues.<br>✓ Define coping mechanisms and identify services and professionals who can provide support. |

| 3. VULNERABLE PERSONS | |
|---|---|
| **General principles** | ✓ Keep your engagement with vulnerable persons to the **minimum required to accomplish your mandate.**<br>✘ Do not engage and collect information from vulnerable persons unless:<br>➤ the information is **strictly required;**<br>➤ there is an **objective added value**; and<br>➤ the same information **cannot be obtained through other sources**.<br>✓ Vulnerability needs to be ascertained individually. **Have specialist/ trained team members conduct a vulnerability assessment and consult with qualified professionals as required**. For persons who present signs of trauma and children, seek the support of a clinical psychologist.<br>✓ The documentation activity **should not take place or should be postponed** if it will cause further harm to the person. |
| **Trauma** | ✓ The impact and consequences of trauma depend on the person but it generally creates long-term psychological, medical and social repercussions.<br>✓ Traumatised persons can reliably convey accurate information. However, trauma can impact on memory.<br>✓ Understand, recognise and be aware of how to deal with trauma.<br>✓ Mitigate risks of re-traumatisation. |

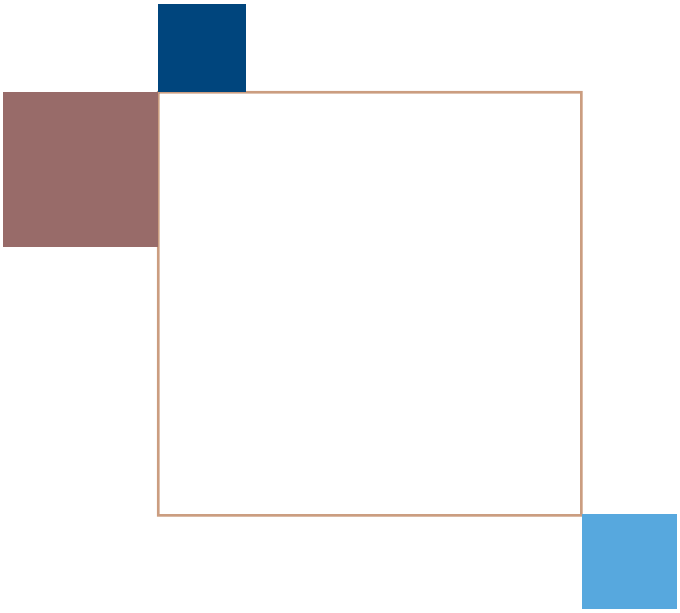
| | |
|---|---|
| **Engaging with vulnerable persons** | ✓ Be empathetic and respectful.<br>✓ Ensure that you are ready to support their physical, psychosocial or other specialised needs.<br>✓ Find out if there are adequate support mechanisms in place to which vulnerable persons could be referred to.<br>✘ Consider whether to refrain from approaching vulnerable persons in the absence of adequate support mechanisms.<br>✓ Assess the person's vulnerability and tailor your engagement according to the potential effects of trauma.<br>✓ If serious indicators of risk exist (e.g. desire to harm oneself), immediately consult a healthcare professional. |

| 4. TAKING A PERSON'S ACCOUNT | |
|---|---|
| **Five guiding principles** | ✓ **Ideally, a person should be interviewed only once with the level of detail required for judicial proceedings. Such interviews should be conducted by the competent investigative authorities.**<br>✓ **To support criminal accountability efforts, there is no need for civil society organisations to take detailed accounts from persons who may have information relevant to potential investigations and prosecutions – especially in relation to vulnerable persons and where the competent investigative authorities are already actively investigating.**<br>➤ Focus your efforts on identifying and locating victims and witnesses, and mapping victimisation and alleged crimes. Pass on this information to the competent investigative authorities for a future interview.<br>✓ **If you determine that it is necessary to take a person's account in pursuit of your mandate, limit yourself to eliciting a first general account, and endeavour to follow good practices.**<br>✘ **Questioning a person already carries risks for the integrity of the person's account, particularly if inappropriate questioning techniques are used.**<br>✓ **Refrain from taking an account from vulnerable persons, in particular from traumatised persons and children.**<br>➤ If you decide to take a first general account from a vulnerable person in pursuit of your mandate, elicit the minimum information required to achieve documentation objectives. Respect the do-no-harm principle and apply recommended best practices. |

| | |
|---|---|
| **General considerations for taking a person's account** | ✓ Question each person separately and individually.<br>✘ Refrain from questioning a person who has already been questioned on the same facts by the same/another organisation or by the competent investigative authorities.<br>✘ Never pay or offer any form of remuneration or any other advantage to a person in return for obtaining an account.<br>✓ Remain professional in your interactions with the person being questioned. Build trust; ensure active listening and a non-judgmental attitude; show empathy (not pity), respect and always keep calm.<br>✓ Use regular breaks to evaluate and discuss with your team the person's demeanour, signs of trauma and distress, and the dynamics of the questioning process. |
| **Planning and preparation** | ✓ Obtain background information on the person being questioned.<br>✓ Enquire whether the person is represented by a legal counsel.<br>✓ Conduct a risk assessment prior to initiating contact.<br>✓ Plan your questioning by defining its objectives and identifying topics to cover.<br>✓ Ensure that all the required conditions for taking a person's account are met, including:<br>➤ trained and experienced interviewers;<br>➤ interpretation; and<br>➤ location, sufficient time, travel panning, equipment and culture-specific logistical requirements<br>✓ Create a safe, caring and private environment.<br>✓ Consider remote questioning only when an in-person interview is not possible. |
| **Engage and explain** | ✓ Explain in detail the purpose and framework of the process.<br>✓ Build a rapport with the person and address their concerns.<br>✓ Obtain biographical details of the person being questioned.<br>✓ Discuss the importance of confidentiality, risks and mitigating measures.<br>✓ Describe the process: types of questions, interpretation, breaks, meals and use of information, e.g. |

| | |
|---|---|
| **Account** | ✓ **Keep the questioning to the minimum required level of detail.**<br>✓ Stop when you have a good general understanding of what the person experienced or witnessed.<br>✓ Initiate the questioning with a **free narrative**.<br>✓ Adopt a chronological structure, where possible.<br>✓ Primarily use open-ended questions and restrict the use of probing/ focused/closed questions to extract details required or to clarify a topic under discussion. Return to the open-ended questions at the earliest opportunity.<br>✗ **Do not ask leading or multiple questions**. Avoid unnecessarily repeating the same question.<br>✓ Keep questioning **neutral, objective** and **factual**, noting the basis on which the person knows the information provided.<br>✓ Maintain a **culturally appropriate behaviour,** including suitable eye contact. |
| **Closing** | ✓ End questioning on a neutral topic and acknowledge the person's participation. Give the person time for closure.<br>✓ Read to the person the summary of your notes on the account, so that any major errors or misunderstandings can be corrected and ask the person if there is any information to add or clarify.<br>✓ Reconfirm informed consent.<br>✓ Assess the process with the person.<br>✓ Reinforce the importance of confidentiality and repeat protection and support measures that can be put in place, as required.<br>✓ Check that the person is well informed of your contact details for future communications. |
| **Evaluation** | ✓ Take time to evaluate:<br>➤ the person's security and well-being;<br>➤ information provided and its contribution to documentation efforts; and<br>➤ performance of those taking the account. |

| | |
|---|---|
| **Documenting the account** | ✘ **Do not produce a signed 'witness statement'.**<br>✓ **Instead, produce a written record of your documentation activity, summarising in it the information obtained as understood by the person(s) taking the account.**<br><u>When producing a written record:</u><br>➤ draft in the third person a summary of what you perceived to be the chronological order of events; and<br>➤ identify and describe in the record any relevant materials the person indicated they have.<br>✘ Do not record your opinions, comments, thoughts or analysis.<br>✓ Ensure the person does not sign the written record.<br><u>Audio/video recording:</u><br>✘ As a general principle, do not audio/video record the process.<br>✓ Where there is a decision to do so:<br>➤ obtain informed consent;<br>➤ test your equipment; and<br>➤ announce the location, date and time, who is being questioned and who else is present in the room. |



| | |
|---|---|
| **Taking an account from vulnerable persons** | ✓ Traumatised individuals and children can be particularly vulnerable and should be questioned only once by investigators with specialised training and experience, working for the competent investigative authorities.<br>✘ Do not take an account from traumatised individuals and from children.<br>✓ Instead, collect the relevant information on such persons and pass it on to the competent investigative authorities at the earliest opportunity.<br>✘ If, in exceptional circumstances, you determine that it is necessary to take a first general account from a traumatised person or a child, make sure to comply with the do-no-harm principle and be prepared and able to follow recommended best practices.<br>✘ **If you are unable to make a vulnerability assessment, do not proceed with the questioning.**<br>✘ **If the person is assessed as not being capable of providing informed consent, or not being fit for questioning, do not proceed.**<br>Follow good practices:<br>✓ Consider the composition and training of the team<br>✓ Seek the support of a psychologist or psychiatrist when taking an account from a traumatised person or a child.<br>✓ Ensure that interpreters and intermediaries are trained and briefed.<br>✓ Consider having a support person involved.<br>✓ Allow vulnerable persons to decide on the meeting location, time and presence of support person.<br>✓ Keep any questioning at a general level and to the minimum necessary. Use questions that are easy to understand.<br>✓ **Only elicit details about traumatic events if really necessary.**<br>✓ Monitor the person's physical and psychological well-being.<br>✓ Suspend the questioning if the person shows signs of distress.<br>✓ Afterwards, conduct an assessment, ideally with the support of a psychologist. |

| | |
|---|---|
| **Victims of sexual and gender-based crimes (SGBC)** | ✓ **SGBC victims might be in a vulnerable condition or even traumatised. Conduct a vulnerability assessment.**<br><br>If you assess that obtaining a first general account from a SGBC victim is required:<br><br>✓ Ensure that those conducting the questioning and interpreters have the required training and experience.<br><br>✓ Adapt your language and references to sex and sexual body parts to the local customs and culture:<br>➤ note the victims' use of particular vocabulary when referring to sexual acts or to certain parts of the human body;<br>➤ use body diagrams; and<br>➤ question the victim about any physical items (e.g. clothes) and medical or forensic information that might have been collected at the time of the assault;<br><br>✓ In relation to male SGBC victims, be prepared to spend extra time building trust and dealing with trauma that might not be immediately visible. |
| **Children** | ✓ **Children (under 18 years of age) should be questioned only once by investigators with specialised training and experience working for competent investigative authorities.**<br><br>✘ **As a general rule, do not take accounts from children.**<br><br>✓ Focus on the child's biographical and contact data and engage with parents/caregivers/doctors to obtain a first general account of what may have happened to the child or what the child may have witnessed.<br><br>If, in exceptional circumstances, obtaining a first general account is assessed to be in the child's best interest and the best course of action, ensure the following.<br>➤ act in the best interests of the child;<br>➤ questioning conducted by persons with recognised expertise;<br>➤ vulnerability assessment performed by a psychologist;<br>➤ informed consent from the child's parent or guardians;<br>➤ engage with and explain process to the child;<br>➤ parents or legal guardians are present where possible;<br>➤ adopt a suitable language for the child's age and development; and<br>➤ mainly use open-ended questions and keep questioning to minimum. |
| **Persons who may have committed crimes** | ✓ Conduct a specific risk assessment.<br><br>✘ Do not actively solicit any information about the person's own involvement in crimes.<br><br>✓ If the person spontaneously volunteers information implicating themselves in a crime, reassess the security situation prior to continuing.<br><br>✓ If and when safe to do so, record any information received and the circumstances of the discussion. Record precise wording used by the person. |

| 5.TAKING PHOTOGRAPHS AND VIDEOS | |
|---|---|
| **Preliminary steps** | ✓ Assess the applicable legal framework.<br>✓ Assess security.<br>✓ Whenever safe and appropriate, seek informed consent of those being photographed/filmed.<br>✓ Select adequate equipment.<br>✓ Create a record of the photo/video documentation process.<br>➤ *See Chain of custody template – Annex 2 to the Guidelines.* |
| **Determine what should be filmed or photographed** | ✓ Capture the **WHAT – WHO – HOW** |
| **How to take videos or photographs?** | ✓ Record the day, time and location of the images **(WHEN/WHERE)**.<br>✓ Take photographs/videos from different views: go from panoramic to wide/medium range shots and close-up shots.<br>✓ Use a ruler (or another object) to indicate dimensions.<br>✓ When filming, state for the record the place, date and time, name of the person(s) filming and any specific persons being filmed. |
| **Preserve the videos and photographs** | ✓ Create relevant metadata for capturing images.<br>✓ Use adequate storage and encryption. |

| 6. PHYSICAL ITEMS | |
|---|---|
| **Core principles** | ✓ Only collect physical items and documents **in exceptional circumstances, when**:<br>➤ official investigators are unwilling or unable to do so;<br>➤ there is a risk that the item or materials will be deteriorated, damaged or lost;<br>➤ the do-no-harm principle can be respected; and<br>➤ you are well informed on the procedures to be followed.<br>✓ Advise those in possession of physical items to preserve and keep them safe, and to hand them over directly to competent investigative authorities at the first opportunity.<br>✓ Record the contact details of the provider and try to obtain consent for the physical item(s) to be handed over to accountability mechanisms. |

| | |
|---|---|
| **Practical tips** | ✓ Photograph items in situ prior to collecting them.<br>✓ Apply strict contamination control measures and select the right packaging and storage procedures.<br>✘ Do not collect physical items than might pose a danger to you or others.<br>✘ Do not use the physical item or try to operate it in any way. |
| **Authentication** | ✓ Obtain and record additional information about the item(s) to establish its authenticity.<br>➤ *See Chain of custody template – Annex 2 to the Guidelines.* |

| 7. DOCUMENTS AND DIGITAL INFORMATION | |
|---|---|
| **Definition and principles** | ➤ Documents can be either **physical items** or **digital information** (data stored or transmitted in a digital format).<br>✓ Do not alter the documents received, regardless of whether they are original versions or copies.<br>✓ Use appropriate methods to minimise changes while preserving digital evidence and document all steps taken to preserve the evidence.<br>✓ Use sterile gloves when handling the documents and take photographs.<br>✓ Be aware of the applicable legal framework and the potential risks involved in receiving or being in possession of certain documents. |
| **Specificity of digital information** | ➤ Wherever possible, electronic devices containing digital data **should be handled by digital forensic experts**.<br>✓ If not possible, collect the **original physical storage media**, applying strict contamination control measures, and keep the device stored safely for further examination by an expert.<br>✘ Do not use or try to explore the data within the device.<br>✓ As a measure of last resort:<br>➤ where it is not possible to collect and preserve the electronic device;<br>➤ but the data contained in it is important and will be lost;<br>✓ secure the assistance of a digital forensics expert to conduct a forensic acquisition of the data. |

| 8. ONLINE INVESTIGATIONS | |
|---|---|
| **Basic standards** | ✓ Consider, at all times, whether you might be in breach of any applicable legislation and whether you are exposing yourself and/or others to unacceptable risks.<br>✓ Conduct a security assessment on the digital landscape before initiating any online activity and define and implement a digital infrastructure that will adequately safeguard any risks.<br>✓ Capture online information in a way that makes it possible to establish the **authenticity** and **integrity** of the information.<br>➤ Collect online materials in their native format or as close to their original format as possible.<br>➤ Ensure to capture, as a minimum, the URL, HTLM source code and a 'screen capture' or 'full page capture' – a screenshot or video of the target web page (depending on the content), with an indication of the date and time of the collector's system.<br>➤ If possible, also capture embedded media files and metadata, contextual data and collection data.<br>✓ Calculate and record the hash value of each digital item.<br>✓ Store items in a new/clean media device. |

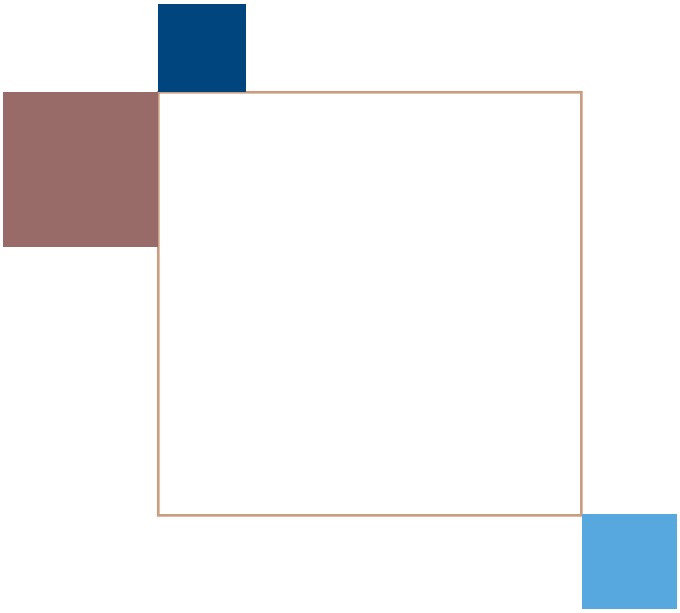
| 9. PHYSICAL INJURIES | |
|---|---|
| **Refer victims to medical professionals** | ➤ **Only qualified medical practitioners can medically examine a victim.**<br>✓ If no such professionals are available, limit your interactions with victims to only document visible injuries.<br>✓ Obtain prior informed consent and keep a record of every action taken.<br>✓ Protect the information collected with a high level of privacy.<br>✓ Encourage and support victims to seek professional medical attention and to preserve all records. |

| 10. CRIME SCENES | |
|---|---|
| **Principles of crime scene examination** | ✘ **Do not enter or disturb the scene in any way and immediately contact the appropriate authorities.**<br>✓ Take available measures to prevent others from contaminating the crime scene.<br>✓ Intervene **only in exceptional circumstances**, namely if:<br>➤ no competent investigative authorities are willing or able to secure the location in a timely manner or, where possible and advisable, they have been notified that such an intervention is under consideration and have assented thereto;<br>➤ not examining the location is very likely to result in crucial information being lost or suffer irreparable damage;<br>➤ you can respect the do-no-harm principle;<br>➤ you have the capability and resources to follow adequate procedures.<br>✘ **Do not proceed if identified risks are assessed to be at an unacceptable level.**<br>✓ Maintain objectivity and impartiality.<br>✓ Maintain the crime scene integrity.<br>✓ Respect privacy and human dignity. |
| **Secure and preserve the integrity of the crime scene** | ✓ Apply strict contamination control measures (e.g. demarcate the site, wear personal protection equipment and limit access). |
| **Document your examination of the crime scene** | ✓ Record all the relevant information (e.g. date and time of arrival, location, individuals present, general description and methodology).<br>✓ Take photos and videos from different views of both the general site and specific aspects, prior to any disturbance of the scene. |
| **Processing the crime scene** | ✘ Do not touch or collect dangerous items; take images instead.<br>✓ Collect items as soon as possible after their discovery has been documented.<br>✓ Establish a safe secure area on site for temporary storage and move the collected items to a permanent secure location when possible.<br>✓ Obtain the contact details and consider questioning some of those present at the crime scene.<br>If faced with human dead bodies:<br>➤ do not touch or disturb the bodies;<br>➤ take photos or videos;<br>➤ collect information as to the identity of the victim; and<br>➤ keep a record of eventual burial. |

| | |
|---|---|
| **Documenting burial sites and mass graves** | ✗ **Exhumations and autopsies should only be conducted by certified practitioners.**<br>✓ Consider reporting the presence of the sites to the relevant authorities.<br>When authorities and forensic experts are not available, limit your actions to:<br>✓ preserving critical information on the burial site;<br>✓ closing or limiting access to the site, and sensitising the local community to the need of securing the site; and<br>✓ recording your findings and the scene through filming or photos. |

| 11. STORING AND SAFEGUARDING | |
|---|---|
| **General principles** | ✓ Conduct a risk assessment in relation to the preservation and storage of the information.<br>✓ Preserve the integrity of every item and the information collected from the moment it has been obtained to the moment when it is handed over to the competent investigative authorities.<br>✓ Keep a thorough and unbroken record of the chain of custody for every piece of information collected.<br>➤ *See Chain of custody template – Annex 2 to the Guidelines.*<br>✓ Create a log or database of the collected information and apply proper information management principles. |
| **Packaging** | ✓ Package every item collected individually to ensure safe keeping and prevent its deterioration.<br>✓ Use appropriate packaging according to the size and nature of the item. |
| **Labelling, sealing and cataloguing** | ✓ Label every package with basic relevant information for easy identification.<br>✓ Use tamper-evident seals, close the package with it, date and sign the seal.<br>✓ Create a document or database recording basic information on all materials collected. |
| **Storage** | ✓ Store all information and items collected safely, using physical or digital storage systems, depending on your resources.<br>✓ Lock, encrypt, anonymise and secure sensitive information and keep it separate from the rest of the collected material.<br>✓ Control access to the information to a minimum and keep on a need-to-know basis.<br>✓ Regularly back up all information collected, make copies and keep them separately.<br>✓ Develop an emergency security plan in case any information is put at risk. |

| 12. ANALYSIS OF COLLECTED INFORMATION | |
|---|---|
| **Core principles** | ✓ **Conduct your analysis in a manner that does not affect the integrity and chain of custody of the collected materials.**<br>✓ Record your analysis separately from the records created to capture the factual information collected.<br>✓ Include clear references to the information or materials used, as well as the methodology employed.<br>✓ The following analysis, in particular when it relates to large data sets, may be particularly helpful:<br>➤ source evaluation (credibility of the source and reliability of the information);<br>➤ contextualisation of the information (connect, link and compare with other information collected); and<br>➤ strength of the information (identify leads and corroboration).<br>✓ Share your analysis with the competent national or international accountability mechanisms, together with the underlying information as soon as possible. |



# ANNEX 4:
# KEY RESOURCES[1]

- Office of the High Commissioner for Human Rights – 'Istanbul Protocol: Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment', 2nd edition, 2022.
  https://www.ohchr.org/en/publications/policy-and-methodological-publications/istanbul-protocol-manual-effective-0

- Global Code of Conduct for Gathering and Using Information about Systematic and Conflict-Related Sexual Violence (the Murad Code), 13 April 2022.
  https://static1.squarespace.com/static/5eba1018487928493de323e7/t/6255fdf29113fa3f4be3add5/1649802738451/220413_Murad_Code_EN.pdf

- Institute for International Criminal Investigations – 'IICI guidelines on remote interviewing', 2021.
  https://iici.global/0.5.1/wp-content/uploads/2021/08/IICI-Remote-Interview-Guidelines.pdf

- Mendez Principles – 'New Principles on Effective Interviewing for Investigations and Information Gathering', 2021;
  https://www.apt.ch/en/resources/publications/new-principles-effective-interviewing-investigations-and-information

- United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh – Trauma-Informed Investigations Field Guide', 2021.
  https://www.unitad.un.org/sites/www.unitad.un.org/files/general/2104429-trauma-informed_investigations_field_guide_web_0.pdf

- United States Holocaust Memorial Museum – 'Pursuing Justice for mass atrocities – A Handbook for Victim's Groups', 2021.
  https://www.ushmm.org/m/pdfs/USHMM-Pursuing-Justice-for-Mass-Atrocities.pdf

- Bournemouth University – 'The Bournemouth Protocol on Mass Grave Protection and Investigation', 2020.
  https://issuu.com/bournemouthuniversity/docs/the_bournemouth_protocol_on_mass_grave_protection_?fr=sMjc3OTI0MjAyNzM

- Office of the High Commissioner for Human Rights/Human Rights Center UC Berkeley School of Law – 'Berkeley Protocol on digital open source investigations', Advanced version, 2020.
  https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

- Global Rights Compliance LLP - 'Basic Investigative Standards for International Crimes', 2019. https://globalrightscompliance.com/wp-content/uploads/2022/03/Basic-Investigative-Standards-for-International-Crimes-Hardcopy.pdf

- Women's Initiatives for Gender Justice – 'The Hague Principles on Sexual Violence', 2019.
  https://4genderjustice.org/ftp-files/publications/The-Hague-Principles-on-Sexual-Violence.pdf

[1] These resources are provided as a support to civil society organisations' further research. Eurojust, the Genocide Network and the Office of the Prosecutor of the International Criminal Court do not necessarily subscribe to all the views and positions contained in such resources.

- United Kingdom Foreign and Commonwealth Office – 'International Protocol on the Documentation and Investigation of Sexual Violence in Conflict', 2nd edition 2017.
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/598335/International_Protocol_2017_2nd_Edition.pdf

- International Nuremberg Principles Academy - 'Cooperation between Civil Society Actors and Judicial Mechanisms in the Prosecution of Conflict-Related Sexual Violence: Guiding Principles and Recommendations', 2017.
  https://www.nurembergacademy.org/fileadmin/media/pdf/projects/improving_cooperation_sexual_violence/Guiding_Principles_And_Recommendations_CRSV.pdf

- Office of the High Commissioner for Human Rights – 'The Minnesota Protocol on the Investigation of Potentially Unlawful Death', 2016.
  https://www.ohchr.org/sites/default/files/Documents/Publications/MinnesotaProtocol.pdf

- Public International Law & Policy Group – 'Handbook on Civil Society Documentation of Serious Human Rights Violations', 2016.
  https://static1.squarespace.com/static/5900b58e1b631bffa367167e/t/59dfab4480bd5ef9add73271/1507830600233/Handbook-on-Civil-Society-Documentation-of-Serious-Human-Rights-Violations_c.pdf

- Witness, 'Video as Evidence Field Guide', 2016.
  https://vae.witness.org/video-as-evidence-field-guide/

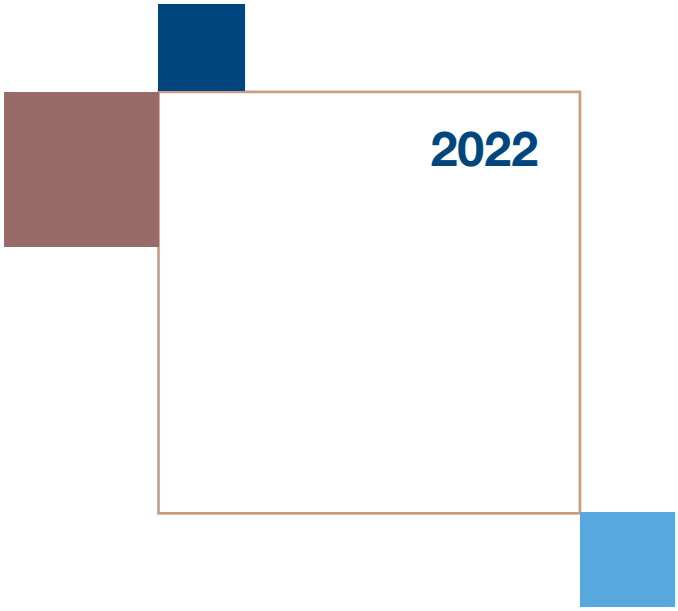
- Institute for International Criminal Investigations – 'Guidelines for investigating conflict-related sexual and gender-based violence against men and boys', 2016.
  https://iici.global/0.5.1/wp-content/uploads/2017/03/160229_IICI_InvestigationGuidelines_ConflictRelatedSGBVagainstMenBoys.pdf

- European Union Agency for Cybersecurity – 'Electronic evidence – A basic guide for First Responders', 2015.
  https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

- Office of the Prosecutor of the International Criminal Tribunal for Rwanda – 'Best Practices Manual for Investigation and Prosecution of Sexual Violence Crimes in Post-Conflict Regions', 2014.
  https://unictr.irmct.org/sites/unictr.org/files/publications/ICTR-Prosecution-of-Sexual-Violence.pdf

- United Nations Office on Drugs and Crime – 'Crime Scene and Physical Evidence Awareness for Non-Forensic Personnel', 2009.
  https://www.unodc.org/documents/scientific/Crime_scene_awareness__Ebook.pdf

- World Health Organization – 'Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies', 2007.
  https://www.who.int/publications/i/item/9789241595681




**CATALOGUE NUMBER** QP-07-22-681-EN-N
**ISBN:** 978-92-9490-808-7
**DOI** 10.2812/682168