

Confidentiality Guiding Note for Referring Protection Cases

It is essential that all parties maintain confidentiality in all cases of abuse, exploitation or violence. Below we outline what that means, why it is important, how to maintain confidentiality, and best practices for sharing information while still guaranteeing confidentiality.

What is confidentiality...

Confidentiality: Conditions under which information revealed by an individual in a relationship of trust will not be disclosed to others.

Identifying Information: Information which can help you work out the identity of an individual. It can include names, age, physical description, location of work, home or school, date of visit, details of the case, names of relatives, etc.

Survivor: A person who has experienced abuse, exploitation or violence. “**Victim**” is typically used, for legal reasons, in judicial and medical sectors. “**Survivor**” is generally preferred by psychosocial support sectors to reinforce the individual’s strength and resilience.

Perpetrator: A person, group, or institution that directly inflicts or otherwise supports violence, abuse and/or exploitation.

Why ensure confidentiality...

Any lack of confidentiality may have negative effects on the lives of survivors and may result in serious consequences for other people involved in the process. Examples of the possible negative impact due to inappropriate information sharing include: 1. During a large meeting someone raised the issue of a gathering of sex workers, naming a venue within a specific town. This non-consensual disclosure could lead to stigmatisation of women. 2. An e-mail sent about a child protection case, where the child was not named, but their siblings were. This e-mail was then forwarded to numerous staff who were not acting on this information, the identity of the child could easily be ascertained and confidentiality breached.

Confidentiality is in the best interest of the person at the centre of the case because it prevents the misuse of information about them for purposes beyond their control, including for their exploitation, stigmatization and abuse, intentionally or unintentionally.

An incorrectly or falsely accused perpetrator could become a victim of hate or slander.

How to maintain confidentiality ...

Information collection...

Conduct discussions in private settings and try not to draw attention to yourselves and those participating, as this may be used later to find out the source of information.

Record group discussions without identifying individual participants’ names, or any other identifying details. Remove pages containing personal information such as names and addresses from notebooks.

Information gathering must be accompanied by support to the survivor, through referral to essential services and further monitoring to ensure there is no negative impact from reporting the case.

Maintaining information...

Substitute names and identifying information with alpha-numeric codes.

In those few instances when it is both appropriate and necessary to record identifying information and details of an incident, it should be stored in a lockable filing cabinet, drawer or room, and the keys kept with the person responsible for the information.

Access to rooms containing paper or electronic information should be restricted to authorised personnel only.

No one else should be given independent access to identifiable information without permission. Information should be kept securely locked when the person responsible for the information leaves the room.

Confidentiality Guiding Note

Managers have a particular responsibility in maintaining the confidentiality of these records and must ensure that the records, or any information they contain, are made available only to relevant parties.

All electronic information on those who have experienced abuse, exploitation or violence should be password protected and the passwords changed on a regular basis.

Destroy computer printouts, written notes, extra photocopies, reports and other records that are not needed, so that they cannot be found and read.

Capacity building...

Include obligations to maintain data protection protocols and ensure confidentiality in staff employment contracts.

Train staff to understand the critical importance of confidentiality during their induction to the organisation.

Develop clear guidelines and procedures for collecting, storing, using, and destroying confidential information. Share these guidelines with all staff joining your organization.

Information sharing...

Information about cases which could jeopardise the confidentiality or well-being of the survivor must never be shared.

The transfer of information - verbally, through the mail, electronically, etc - should be done in such a way that confidentiality is maintained.

Paper files should be transferred by hand between people responsible for the information. During transfer files should be stored in a sealed box or sealed envelope.

Electronic information should be transferred in encrypted or password protected format. Memory sticks should be passed by hand between people responsible for the information and the file erased immediately after transfer.

When verbally sharing information, ensure it happens one-on-one, not in a large group, and is in a private space where you cannot be overheard. Do NOT share information in group meetings.

Who can you share with...

Survivors are the ones who can say who can have information, when and how. They should be given the opportunity to highlight any information that they do not want any particular person to know. (For example, they may not want their family to be told personal details about them that they would rather communicate face-to-face.)

Sharing of information (which could identify a survivor, an individual involved in a case, or an alleged perpetrator), should be purely on a 'need to know' basis. It should only be shared with other personnel or agencies who will do something to provide direct support to the survivor or who will action something as requested by the survivor (e.g. not every CP actor needs to be informed of the details of every CP incident).

Information sharing lines must be clearly mapped out and understood by all staff. Passing information between different agencies requires that all agencies concerned comply with the standard information protection protocols.

After gathering, information should be passed only to a person designated to receive it for clearly defined reasons, such as a line manager or partner agency Protection staff who will be taking action.

Keep the number of people informed of the case to an absolute minimum. The fewer people involved the easier to ensure client confidentiality.