MODULE 18

Filing Systems and Document Management

Lawyers and NGOs working on torture cases must have in place effective systems for document management. It is helpful to have a file management structure that is uniform across the organisation that allows current and future members of staff to navigate and locate files easily. Some organizations may use online case management or cloud-based storage tools to assist with document management and storage.

1. Document Management

Filing Systems: If possible, electronic copies of all documents should be kept so that files are not lost. Electronic files are often less vulnerable to seizure. If using online tools for document management, ensure these meet the necessary security requirements.

Setting up Folders and Subfolders for each Case: where files are stored electronically, case files can be arranged as follows containing subfolders: (i) Admin; (ii) Background documents; (iii) Correspondence; (iv) Submissions; (v) Decisions; and (vi) Implementation.

Agreeing a Naming Convention for Documents: It is useful to agree a naming convention for documents **E.G.,** *Date (year/month/day) - Case Name - Short title – Initials of Author.doc – Multiple Drafts.com.*

Regular Review of Documents: It is useful to regularly review documents in a case file to ensure that they are saved correctly and there is nothing missing in the case file.

2. Managing Correspondence

All communications should be conducted safely and securely. Contact with survivors should be maintained throughout a case, even during periods of inactivity. Organisations should keep a record of all communications with survivors, particularly where advice or instruction is being given, or strategy is being discussed with partners or other lawyers.

Communication in Person or over the Phone: Keep a record of all communications – if in person, or over the phone, meeting notes can be taken to briefly summarise the communication and any action agreed upon.

Correspondence via Email: Cloud-based systems that allow for automatic filing of cases are helpful and, even where automated systems do not exist, all email communications should be copied to the case file for accurate records.

Correspondence via Post: All letters should be scanned and saved in the electronic case file. Maintaining a scanned copy will suffice and the original letter can be discarded, unless the original document is not replaceable, **e.g.,** a notarized affidavit or a stamped court document.

Correspondence with Courts and Tribunals: Substantive correspondence should be sent in a formal letter, which can be sent electronically by email and should be sent in accordance with the rules of procedure of the relevant court or body, **e.g.,** the ACHPR now accepts documents in electronic version only (sent by email). The court's practice directions should be reviewed for any specific format requirements for correspondence and written pleadings, **i.e.,** some require communications must be made using specific forms.

3. Managing and Collecting Evidence

The collection of evidence will often involve several partners – particularly where the case is outside your jurisdiction – and it is critical that logistical issues associated with building an evidentiary base are factored into the process early.

When conducting interviews, the following should be considered:

- **Preparation:** what is the information you are seeking to obtain?
- **Logistics:** interviewees should feel comfortable and safe
- **Language**: you may need an interpreter which will require planning and budgeting in advance
- **Confidentiality:** must explain how their statement be used and how will they be protected
- **Location:** consider whether the interviewee feel safe and at ease
- **Recording and storage:** seek consent and ensure you have the means to safely store the data
- **Special arrangements**: interviewers must have the knowledge and skill to conduct interviews
- **Other considerations:** this may include *inter alia* how trauma will impact the interviewee; medical or psychological support presence; fears of reprisal; ensuring the safety of the person

Further, all evidence must be properly named and filed in the case folder and, if in a language other than the language in which the submission is being drafted, the files should be translated. Collecting or storing evidence may also present security risks for both the survivor and the organisations and so risks should be evaluated, addressed, and mitigation measures adopted.

4. Case Logging and Litigation Calendars

In addition to saving documents and recording communications, it is useful to track significant movements in a case using a Case Log. Logs must be regularly updated and can include information such as: (i) staff assigned to the case; (ii) survivor contact information; (iii) case background information; (iv) violations/crimes; (v) submissions made; and (vi) and next steps. Recording and meeting deadlines is crucial; a deadline missed could deprive a survivor of their only chance to obtain justice, truth, and reparations. It is useful to record deadlines across

cases in a shared calendar so that organisations have clear overview of workload and can plan accordingly.

5. Closing a Litigation File

A case file should be closed in a way that ensures that all data related to the case is handled in accordance with legal and ethical obligations, and in compliance with any applicable jurisdictional data regulation rules.

When to close a case: The criteria to be considered when closing a case mirror those used as the beginning of a case, **i.e., mandate and expertise**, **survivor considerations**, **case considerations**, **case strategy**, **impact**, and **organizational/resource considerations**.

Closing a Case: A letter can be sent to the survivor explaining the arrangements for storage and/or destruction of their file. Electronic files should not be immediately destroyed to protect against any risk of legal action that could be taken regarding advice given.

Consent: Files should not be destroyed without the client's consent. Where you do not have consent to destroy the file, a balance will need to be struck between the ongoing cost of storing files and the risks attached to destroying them (**e.g.,** that the client will want the file back or will bring a claim or complaint).

Digital Security for Effective Case Management

1. General Principles for Digital Security

Prevent: Design and implement a **data breach prevention plan**. This process should include training on steps and procedures for handling a potential breach and mitigating the impact on survivors' privacy and security.

Protect: Online case management or cloud-based storage tools should meet the necessary security benchmarks for the work they are doing. They should be supported by trusted suppliers, configured to reduce security breaches, administered in a secure and accountable manner, and that security vulnerabilities can be identified in a timely manner.

Respond: Once aware of a data breach, you should assess the type of data compromised by the breach, impacted groups, the potential harm to them as a result of the breach and implement a recovery plan to redress damage incurred.

2. Outlining and Understanding Risk

When assessing security risks, lawyers and NGOs should consider:

- What are the most crucial information technology resources?
- What type of data breach would significantly impact our work?
- What are the sources of the threats and the potential impact of each identified threat?
- What level of risk are we comfortable taking when dealing with sensitive and confidential information provided by survivors?

3. Safe Communication and Information Sharing

General Practice: When sharing sensitive information, the following actions can be considered:

- Use confidentiality notices or disclaimers when sharing confidential information by email.
- Exercise caution when accessing emails, links, or attachments from unfamiliar sources.
- Using encrypted platforms, such as Tresorit, Proton mail, or digital share systems, such as Office 365 sharing or Dropbox, to share documents.

Enhanced Security Measures: To increase the protection of communications and information, lawyers and caseworkers can:

- Use project code names when discussing project information with external parties
- Use end-to-end email, encrypted file sharing and encrypted messaging and voice apps
- Use passwords for sensitive Zoom meetings
- Use private and secure messaging systems such as Signal, and consider activating disappearing messages
- Conduct face-to-face meetings and turn off phones or leave them outside the meeting room
- Clean your phone and laptop's desktop and recycling bin when travelling
- Protect sensitive documents by adding passwords
- Provide printouts of documents whenever the security situation demands it
- Use a Microsoft Document inspector to remove metadata where safety is at risk
- Use anonymous social media accounts for researching people of interest
- Use 'incognito'/ 'private browsing' to protect your history and cookies when researching

Preparing for and Managing Breaches: A strategy to mitigate harm caused, report obligations, assign responsibilities and provide access to redress and compensation when required must be put in place.

Compliance: Staff must be aware of the obligations of data protection when they collect or handle data subject regional/domestic standards in their jurisdiction, **e.g.,** EU organisations are required to collect and process personal data in accordance with their responsibilities under the GDPR.