

ADDRESSING SEXUAL HARASSMENT IN CANADIAN MINING

MANAGING INFORMATION AND MAINTAINING CONFIDENTIALITY

Effective management of sexual harassment and/or gender-based violence concerns, incidents, reporting and resolution data involves the collection and management of sensitive and confidential information.

Attention to this important aspect of sexual harassment complaints procedures helps build confidence in the system, offers parties a sense of safety and security and contributes to data creation for the purposes of prevention as well as monitoring and evaluation of related procedures and their impact.

Supervisors and HR professionals may find these tips helpful to collect and manage sensitive information and protect confidentiality relating to complaints of sexual harassment and/or gender-based violence:

1. Collecting Sensitive Information

- **Maintain confidentiality** – make every reasonable effort to ensure that the privacy of the persons involved in a complaint is protected. Share information internally strictly on the basis of who needs to know what. Maintaining confidentiality is subject to the overriding responsibility of investigating and resolving complaints.
- **Act in accordance with applicable legislation and regulations** while also applying trauma-informed approaches. All parties to a harassment complaint are expected to respect the privacy and confidentiality of all other parties involved and to limit the discussion of a complaint or incident to those who need to know.
- **Be informed** – Know your operations and relevant company policies, codes of conduct, file management and data security protocols.

- **Ask only for what you need**, such as specific details relevant to the incident including dates, times, locations, persons involved. It is not necessary to collect extraneous or sensitive information that does not directly pertain to the investigation, as this could compromise the privacy of individuals involved and increase the risk of unauthorized disclosure. Remember to minimize your risk, while managing responsibility for all data.
- **Vary information collection options** – use appropriate channels and diverse tools (e.g., email, phone, video call, or face-to-face meeting) depending on the urgency, complexity, and sensitivity level.
- **Keep track** – classify contents and record the date of every exchange, conversation, meeting, attendee, decision, etc. Also, document how and where data will be stored.
- **Be transparent** – share what types of information will be collected and how data will be protected, stored, kept confidential or shared/not shared with subjects of harassment/alleged perpetrators/witnesses.

2. Using and Sharing Sensitive Information

- **Provide training** – ensure HR and any other staff with responsibility for harassment concerns or data access are trained in proper and respectful, trauma-informed collection and use of sensitive data.
- **Be respectful** – share only relevant, accurate details in a formal, trauma-informed professional tone that respects the feelings and rights of those involved, use compassion and tact.
- **Obtain consent** – ask for consent, feedback, or confirmation when necessary.
- **Support a positive reporting culture** by transparently communicating the information that will or will not be shared with parties concerned throughout the different steps of a formal complaint process.

3. Storing Sensitive Information

- **Establish a procedure for managing files and documentation** related to reports of concern and/or formal complaints, including addressing the points below:
 - Content and evidence that make up an incident or complaint file, including notes, photos and any reports related to a complaint, may be filed in a Human Resources (HR) harassment complaint area or directory, separate from personnel files.
 - Maintain harassment complaint files within human resources/a designated department.
 - Select an appropriate, reliable storage format, deciding whether paper or electronic records would work best.
 - Manage the data life cycle by planning for the collection, use, storage, and destruction of records, in keeping with file management procedures.
 - Limit access by setting requirements and controls for who can access sensitive information. Consider the use of confidentiality agreements for data access.

- Maintain security, ensuring that physical and electronic records of sensitive information are stored securely. Separate sensitive HR information from other company data, including how to handle investigation notes versus the final report, the complaint letter, and what goes into personnel files compared to what stays in the incident, complaint or investigation files.

Physical Data Storage and Safeguards

- Safeguard cabinets/drawers/desks where confidential physical files are stored.

Electronic Data Storage and Safeguards

- Safeguard applications, databases and servers that house and process HR data by using firewalls; installing intrusion detection systems; and, limiting who has the authority to assign passwords.
- Protect stored data by using encryption. Protect in-transit data (e.g., data that pass through a web portal or company network) by requiring a Secure Sockets Layer (SSL) connection for access.

4. Data Destruction

- ***Discard data once it is no longer needed***, in keeping with record retention and destruction policies.
- ***Keep data stored securely*** until it can be discarded.
- ***Be mindful that digital data is difficult to permanently erase!*** Sometimes data can be recovered using advanced tools.

5. Data Breaches

- ***Establish a process to take action*** in the event of a breach of sensitive information.
- ***Report any breaches or issues*** affecting the privacy and security of sensitive information.
- ***Evaluate security measures*** in the event of a data breach and enact needed changes.

References

Government of Canada. (2021). Guide on Applying the Harassment Resolution Process.
<https://www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/harassment-violence/guide-applying-harassment-resolution-process.html>