

AD-ROIT LINKS newsletter

*IN THIS ISSUE

**POSH INQUIRIES AND DATA PROTECTION:
BALANCING EVIDENCE, FAIRNESS AND
CONFIDENTIALITY**

Balancing fair PoSH inquiries with data protection through focused evidence collection, confidentiality and secure handling under the forthcoming DPDP framework.

FROM THE Founder's Desk



Dear Readers,

Welcome to the October edition of **AD-ROIT LINKS**.

As we navigate an increasingly complex regulatory landscape, this month we turn our focus to a critical intersection in modern workplaces: **POSH Inquiries and Data Protection**. With the **Digital Personal Data Protection (DPDP) Act, 2023** and the **DPDP Rules, 2025** being enforced in a phased rollout over an 18-month period, culminating in full enforcement on **May 13, 2027**, understanding how to navigate both laws has never been more urgent.

For HR professionals, Internal Committee (IC) members, and compliance leaders, mastering this dual navigation is essential. POSH inquiries inherently require handling highly sensitive personal data, sensitive personal information, and intimate testimonies. Striking the right balance requires gathering sufficient evidence and ensuring procedural fairness while strictly upholding confidentiality without violating strict data protection mandates, fiduciary duties, and potential penalties under the DPDP framework. Navigating these overlapping obligations demands both legal precision and profound empathy, and our lead discussion unpacks best practices for compliance and governance.

We are also thrilled to introduce an exciting new addition to our publication starting this month—a **Guest Column**. Moving forward, we will be featuring insights from some of the brightest legal minds, esteemed academicians, and distinguished members of the judiciary to help us decipher complex laws and evolving compliance frameworks.

For our inaugural guest column, it is an absolute honor to feature **Dr. Kriti Parashar**, an accomplished academician and professor at Christ University, Ghaziabad, who shares her invaluable perspective with our community on **AI tools and POSH Inquiries: Balancing Employer Liability and Party Confidentiality**.

We hope you enjoy reading this edition and that you find these resources beneficial to your professional journey. After all, empowering you to make the best use of our resources is what **AD-ROIT LINKS** stands for: **resourcefulness**.

Warm regards,

Leeza Dutta Singh

Founder & Managing Partner,
AD-roit LinkS



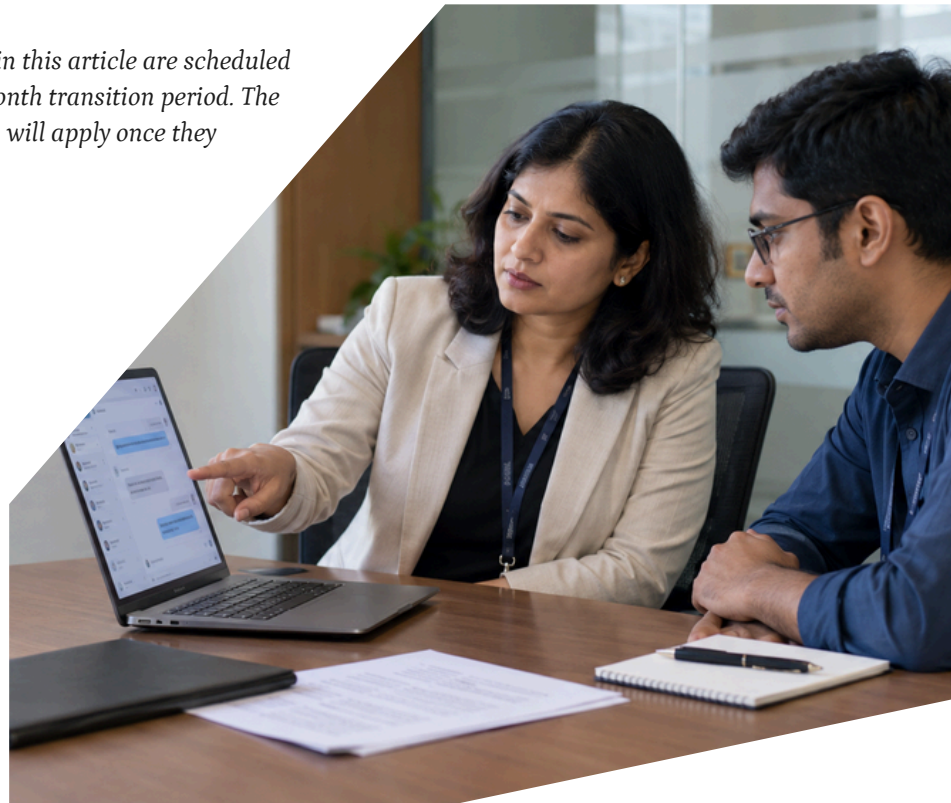
PoSH Inquiries and Data Protection

~ BY ATRYEE DUTTA

Balancing Evidence, Fairness and Confidentiality

(Note: The substantive DPDP provisions discussed in this article are scheduled to take effect on 13 May 2027, after the eighteen-month transition period. The DPDP analysis below explains how these provisions will apply once they commence).

Consider a familiar situation in an Indian company. A sexual harassment complaint reaches the Internal Committee (IC). The committee asks for WhatsApp chats, messages and CCTV footage to understand what happened. Soon, its inbox is flooded with screenshots, personal voice notes, six months of conversations and hours of footage showing employees who have nothing to do with the complaint.



For HR and the committee, collecting more material may feel like being thorough. **Section 11(3) of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (POSH Act), gives the IC specified civil court powers for its inquiry.** These include summoning and enforcing attendance, examining a person on oath, and requiring the discovery and production of documents.

But the power to seek evidence has a purpose. It is meant to help establish the facts of the complaint. It does not give the committee unrestricted access to an employee's digital life.



Under the Digital Personal Data Protection Act, 2023 (DPDP Act), the employer will ordinarily be a Data Fiduciary where it determines the purposes and means of processing. The IC's statutory role and the exemptions available for its inquiry must be considered separately.

The privacy question begins with what happens to this material. Who collects it? Who can see it? Where is it stored, and for how long?

A chat screenshot or CCTV clip may reveal more than the incident under inquiry. It can also contain personal information about colleagues, family members and people who have no role in the complaint.

The employer and the IC therefore need to handle evidence in a way that supports a fair inquiry and protects confidentiality. The forthcoming DPDP framework adds obligations that must be considered alongside the POSH requirements.

The answer is to collect what the inquiry needs, keep it reliable and secure, and share enough for the parties to respond fairly. Unrelated personal information deserves protection throughout.

Where the PoSH Act Meets the DPDP Framework

A question often follows:

Do we need the employee's consent before looking at corporate emails, Slack or Teams messages, WhatsApp chats or CCTV footage?



The answer depends on the purpose of the processing and the legal provision that applies.

Consent and Certain Legitimate Uses

Section 6 sets the standard for consent when consent is the applicable processing ground. It requires a free, specific, informed, unconditional and unambiguous choice, expressed through clear affirmative action and limited to personal data necessary for the specified purpose.

Consent is one route under the DPDP Act. Before asking for it, the employer and the IC should identify what information they need, why they need it and which statutory provision supports that use.

Section 7(i) permits certain processing for employment purposes or to safeguard the employer from loss or liability. This includes preventing corporate espionage and maintaining confidentiality. Processing needed

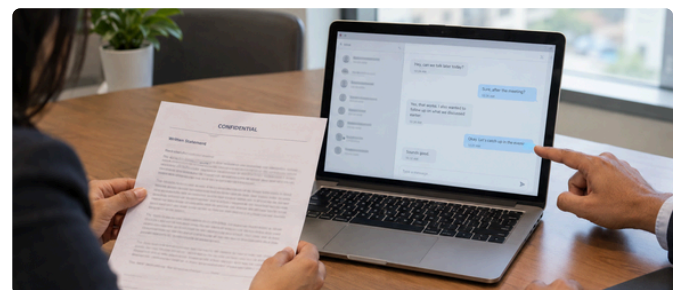
to deal with a workplace complaint may fall within this provision, depending on the facts. Section 7(a) has a different scope: it concerns data voluntarily provided for a specified purpose where the individual has not indicated that they do not consent to that use. It is not a general provision for all employment or compliance activities.

Section 17(1)(b) provides a limited exemption where processing by a body legally entrusted with judicial, quasi-judicial, regulatory or supervisory functions is necessary for those functions. The IC's statutory inquiry mandate and specified civil court powers provide a strong basis for considering this exemption for necessary inquiry processing. This is a legal assessment, rather than an express provision naming every IC or exempting every employer activity. Section 17(1)(a), concerning processing necessary to enforce a legal right or claim, may also be relevant. Where Section 17(1) applies, the exemption covers specified provisions; obligations under Sections 8(1) and 8(5) remain. POSH confidentiality and fair procedure also continue to apply.

This distinction matters in practice. An exemption for necessary inquiry processing cannot simply be carried over to unrelated HR uses, unrestricted searches, public circulation or a vendor's independent reuse of testimony.

Suppose the complaint concerns an incident in October. The IC should begin with records relevant to that incident and enough surrounding context to understand it. If the allegation involves a pattern of conduct, a longer period may be justified. The reasons for expanding the search should be recorded.

An employee's involvement in an inquiry does not make every private conversation relevant to it.



Screenshots, CCTV and Corporate Messaging

Digital records can help the IC understand the sequence of events and test what the parties and witnesses say. Their value depends on context and reliability. Three common sources require particular care.

WhatsApp and Personal Chat Screenshots

A screenshot can be useful, but it needs context. Where did it come from? Is the conversation complete enough to understand the exchange? Has anything been cropped or altered? The IC should consider these questions along with any supporting material.



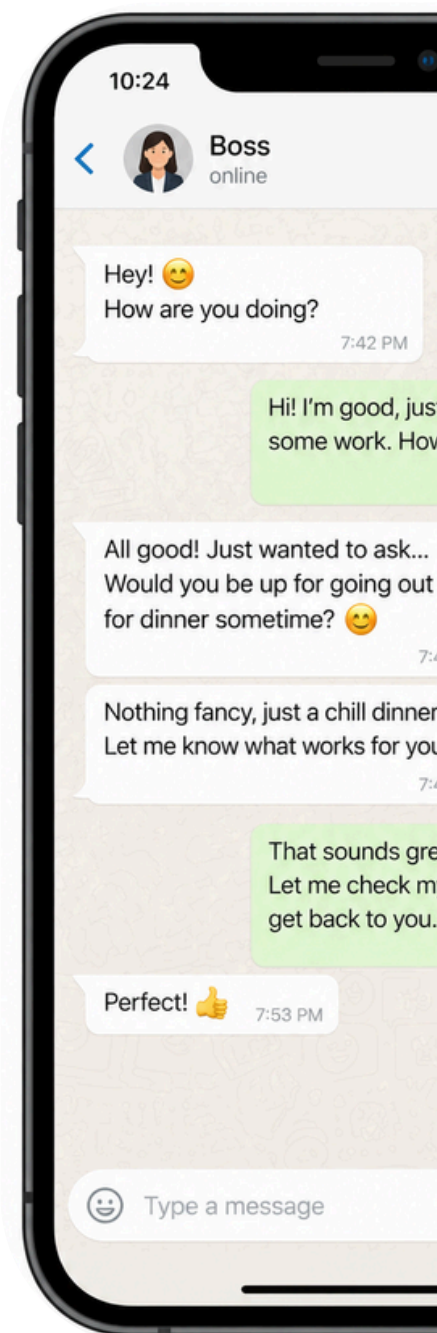
Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), addresses the admissibility of electronic records in proceedings to which that legislation applies.

An IC should not automatically treat a Section 63 certificate as the sole gateway to considering electronic material in a workplace inquiry. The applicable service rules, fair procedure and the reliability of the evidence require attention; the usual standard in a disciplinary inquiry is the preponderance of probabilities.

Preserve the relevant source records, available metadata and details of how the material was obtained. Record who handled it and when. Give the parties an opportunity to question its authenticity and respond to those concerns. A screenshot or chat export, by itself, does not settle whether the material is genuine.

A personal chat export may contain far more than the disputed exchange. Family photographs, unrelated conversations and information about other colleagues can easily find their way into the inquiry file.

Ask for enough of the conversation to understand what happened. Keep relevant originals secure and limit access. Where appropriate, prepare a separate copy for disclosure with unrelated personal details masked. Record what was redacted and why. Information needed to understand or challenge the evidence must remain available.



Workplace CCTV Footage

CCTV can help clarify what happened in a hallway, cafeteria or reception area. It does not always tell the whole story. The IC should check the timing, continuity, surrounding context and any limitations in what the camera captures.

Footage also captures people unrelated to the complaint. Rule 7(2) of the POSH Rules, 2013 requires the complaint copy to be sent to the respondent within seven working days, and Rule 7(4) requires an inquiry consistent with natural justice.

Disclosure of relied-upon footage must provide a meaningful opportunity to respond, with reference to applicable service rules.

The risk arises when raw footage is circulated without limits. That can expose the identities and movements of employees who have no connection with the complaint.

The IC should assess whether masking unrelated faces, limiting the clip or arranging controlled viewing will protect privacy while preserving a meaningful defence. Blurring is a practical safeguard, not a universal statutory requirement. Supervised viewing is appropriate only where it gives adequate access to examine and answer the evidence; copies or further access may still be required by fair procedure or applicable rules.

Enterprise Collaboration Tools

Another assumption is that ownership of the IT system gives management the right to read any employee's inbox or direct messages. Ownership alone does not answer the privacy or procedural questions.

A search should have a clear purpose, written limits and appropriate authorisation. It should be carried out by authorised personnel, with a record of what was accessed and IC oversight where appropriate. Unrelated private conversations should stay outside the review.

A focused written requisition to IT or Information Security is a useful operational safeguard. It should identify relevant custodians, search terms, date windows and the authorised scope, with reasons for any expansion. These details are recommended controls; Section 11 does not prescribe a mandatory IT requisition template. The IC's statutory authority and independence should guide the process.



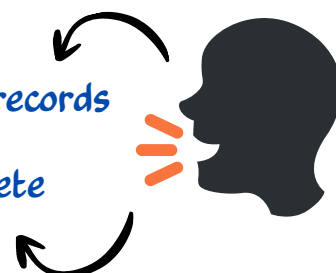
Data Principal Rights during an Inquiry

The DPDP Act provides individual rights within defined statutory limits. Their application to employment and inquiry records depends on the processing basis and any applicable exemption.

Two requests commonly bring this issue into focus:

Delete my inquiry records

Give me the complete inquiry file



Each needs a response based on the applicable law and the purpose for which the records are held.

Erasure and Necessary Retention

Section 12 provides rights to correction, completion, updating and erasure for personal data whose processing was previously consented to, including consent referred to in Section 7(a). It does not give an unconditional right to erase every employment or inquiry record. If someone disputes a statement, preserve the original and place the correction, objection or rebuttal alongside it. The record should show both.



An Erasure Request Requires a Reasoned Assessment

An erasure request does not automatically require deletion of an inquiry file. Section 8(7), where applicable, permits retention necessary for compliance with law, and Section 12(3) recognises necessary retention for the specified purpose or compliance with law. Sections 17(1)(a) and 17(1)(b) may also be relevant to necessary legal-claim or statutory-function processing. Section 18 of the POSH Act provides a ninety-day appeal period; it does not prescribe the complete retention period for

every inquiry file or establish that all legal challenges end after ninety days. Retention should reflect applicable service rules, pending or reasonably anticipated proceedings, legal holds and a documented review schedule. Neither automatic deletion after ninety days nor indefinite retention is appropriate.

Access and Confidentiality

Section 11 of the DPDP Act concerns specified information about personal-data processing where consent was previously given, including consent referred to in Section 7(a). It includes a summary of personal data and processing activities, and specified information about other Data Fiduciaries and Data Processors with whom data has been shared. It is not a general entitlement to the entire inquiry file. Assess its statutory scope and any applicable Section 17 exemption before responding.

Section 16 of the POSH Act restricts publication or communication of protected complaint and inquiry information to the public, press and media. It must be read alongside the Act's required disclosures and fair-process obligations. Confidentiality does not justify withholding relied-upon evidence merely because it contains a witness account.

Rule 7(2) addresses transmission of the complaint copy, Rule 7(3) addresses the respondent's reply and supporting material, and Rule 7(4) requires natural justice. Disclosure of replies, witness accounts and other relied-upon material must allow each party to answer the case under applicable service rules and fair procedure. Section 11(1) also contains hearing and findings safeguards where both parties are employees, and Section 13(1) requires the findings report to be made available to the concerned parties. Any redaction or restricted access should be justified and preserve a meaningful response. Internal deliberations do not become automatically disclosable simply because a DPDP request is made, but a blanket ban on access to witness testimony is equally unsound.

Security Safeguards and Third-Party AI Tools

Consider an IC conducting an urgent virtual hearing with a witness. To save time on the minutes, a committee member or HR coordinator adds an AI transcription bot to the call. Depending on its settings, the tool may record, transcribe and store confidential testimony, including deeply personal accounts, on a third-party provider's servers.

The intention may be administrative convenience. Yet a few clicks can place confidential inquiry material with an external service before anyone has checked who can access it, whether it may be reused or how long it will be kept.

That decision needs a closer look at both confidentiality and security.

Confidentiality requires attention to the provider's role, authorisation, access and use of the material. External processing is not automatically the same as prohibited public disclosure under Section 16, but uncontrolled sharing or reuse can compromise the confidentiality of the inquiry.

Under the forthcoming DPDP framework, Section 8(5) requires reasonable security safeguards where applicable, including when Section 17(1) is relied upon. Using an unassessed tool that retains testimony, exposes it to unauthorised users or reuses it for model training creates a serious risk. Where a provider acts as a Data Processor and Section 8(2) applies, a valid contract is required; an inquiry exemption must not be assumed to cover the provider's separate commercial uses.

The same concern arises in routine file management.

An inquiry file left in an open Google Drive folder, a shared HR SharePoint location or a lengthy email chain can reach people who do not need to see it. An IT administrator or HR colleague handling routine work may then come across witness statements, personal photographs or other confidential material.

Organisations should prohibit unapproved AI transcription tools in IC hearings. Any approved service should undergo privacy and security assessment covering processing purpose, contractual restrictions, model training, access, storage location, retention, deletion and incident response. This is a recommended control, not an express statutory ban on every AI tool.

Inquiry records should be held in secure repositories with access based on documented need and authority. IC members require appropriate access; limited access may also be necessary for authorised custodians, technical support, the employer's statutory action, concerned parties or legal proceedings. Such access should be controlled, logged and subject to confidentiality obligations. Encryption and multi-factor authentication are practical safeguards, rather than provisions expressly requiring exclusive access by active IC members.

A Five Step Evidence and Privacy Protocol

A practical SOP should help the IC make these decisions consistently. The following five steps should be adapted to the applicable service rules, the facts of the case and the basis for processing.

1. Define Scope and Preserve Relevant Evidence.

Record the allegation, necessary data sources, processing basis and authorised collection scope. Avoid routinely collecting entire accounts or lengthy unrelated exports. Where unsolicited material arrives, screen it securely and preserve relevant context and potentially material evidence before disposing of unnecessary copies.

2. Plan Fair Disclosure.

Identify the material each party needs to answer the case. Mask unrelated details where appropriate, retain originals and record the reasons for restrictions. Neither redaction nor supervised viewing should prevent a meaningful challenge to relied-upon evidence.

3. Control Storage and Access.

Use a dedicated repository with appropriate encryption, multi-factor authentication, access logs and secure transfers. Authorise access by role and need, including lawful disclosure and necessary technical support; review permissions when membership or responsibilities change.

4.

Govern Hearings and External Tools.

Prohibit unapproved recording and transcription services. State the recording arrangements in advance, assess any approved provider and restrict reuse and onward disclosure. Secure minutes or an authorised recording can be used where justified; neither personal recording nor locally stored recording should be assumed lawful or unlawful solely because of its format.

5.

Review Retention and Disposal.

Preserve the evidence and procedural record needed for the inquiry, appeal, legal obligations and pending or reasonably anticipated proceedings. Apply documented legal holds. Review retention after these needs cease, retaining any record still required and securely deleting unnecessary extracts and duplicates. Ninety days is an appeal period, not an automatic deletion deadline.

Where Workplace Dignity Meets Data Protection

A workplace complaint places people in a vulnerable position. The complainant needs a credible process, the respondent needs a fair opportunity to answer, and witnesses need confidence that their information will be handled responsibly.

The employer's role is to give the IC the systems and support to do this properly. Focused evidence collection, secure storage, fair disclosure and a reasoned retention policy should be part of how the inquiry is run.

Before closing the file, the IC should be able to explain why the information was collected, who received it, how it was protected and why it still needs to be retained. That discipline helps protect the people involved and strengthens the credibility of the inquiry.



AI tools and PoSH Inquiries:

Balancing Employer Liability and Party Confidentiality

ABOUT THE EXPERT



Dr. Kriti Parashar

PoSH trainer, IC Member and Assistant Professor, CHRIST (Deemed to be University), Delhi NCR

Dr. Kriti Parashar is a legal academic, certified POSH trainer, trained mediator, and Internal Committee member at CHRIST (Deemed to be University), Delhi NCR. Her expertise spans gender justice, workplace sexual harassment, constitutional law, and Internal Committee procedures, with a focus on promoting diversity, inclusion, and effective workplace compliance.



► Q. How do AI surveillance, transcription, and summarization tools impact Employer Liability and IC Confidentiality under POSH and DPDP?

Employers deploying algorithmic monitoring like email scanners, keystroke loggers, or facial recognition must comply with the Digital Personal Data Protection (DPDP) Act, 2023, which designates them as Data Fiduciaries. Under Section 6, invasive AI tracking without an itemised notice and "free, specific, informed, unconditional, and unambiguous" consent is illegal. Section 7 restricts data usage strictly "for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary". Furthermore, Section 8(1) mandates that data used for decisions affecting individuals must be complete, accurate, and consistent. Using automated AI tools to decide cases conflicts under this regulatory regime violates the strict confidentiality required by Section 16 of the POSH Act.

Under Section 8(5), employers are legally liable for data leaks, even if caused by a third-party AI Data Processor. When Internal Committee (IC) members use unvetted tools (like Otter.ai, Zoom AI Companion, or Teams Premium Transcribe, etc.) they may breach this safety mandate. These cloud platforms transmit highly sensitive testimonies to external servers, and many public models retain inputs to train their algorithms, removing the data from the IC's absolute control. Finally, if an employee exercises their Right to Erasure under Section 12 of DPDP, employers will find compliance technologically impossible once the data is absorbed by an AI training model.

▶ Q. How can the IC members and Employers ensure compliance with DPDP and PoSH as regards AI tools usage?

A robust Confidentiality and AI Protocol Clause within the IC handbook acts as a legal firewall, translating the absolute privacy mandates of Sections 16 and 17 of the PoSH Act into clear operational rules. It can explicitly state:

“

No member of the IC, complainant, respondent, witness, or accompanying individual shall introduce, deploy, or utilize any third-party Artificial Intelligence software, automated productivity tools, or cloud-based applications during physical or virtual hearings. All evidence submitted, minutes of meetings, and final reports must be recorded manually or via secure, corporate-approved, air-gapped (offline), or locally installed enterprise systems that guarantee zero data retention and explicitly ensure that data is not used for external algorithmic training.

By defining unauthorized digital disclosures, this clause removes ambiguity, shields the organization from severe litigation, protects participants from data leaks, and preserves inquiry integrity. Further, to ensure compliance, a Notice of Digital Personal Data Processing and Explicit Consent Pursuant to the DPDP Act, 2023 must be integrated into communications, establishing the employer as a compliant Data Fiduciary. The notice can read:

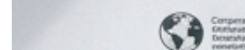
“

You are requested to participate in an official inquiry proceeding conducted by the Internal Committee (IC). For this purpose, [Company Name], acting as the Data Fiduciary, needs to collect, record, and process your personal data, including your verbal testimony, written statements, and any digital evidence submitted by you or third parties. In compliance with Section 7 of the DPDP Act, 2023, your data will be used strictly and exclusively for the determination of the current PoSH inquiry.



The notice can be accompanied with duties of parties to “not deploy any AI tools to generate evidence or digital interception tools during the inquiry process.” A similar duty can be added for the IC that it guarantees that —

- ✔ No external, unvetted AI tools or third-party cloud processors will be utilized to record, transcribe, or analyze your data. (and if any being used to be mentioned) and,
- ✔ Your data will not be repurposed for broader corporate surveillance, performance analytics, or external software model training.”



AI Protocol

protocol

behavior agreement and autonomous
and samdity orais and the call
of and their colors.

av out and under the pronw
protocol may imay to minoue to

al: secess and undor's teamir

regndy row and the numin
and contaue abe dissonitdar

e to me for understernat
; apess, snawen-line edard
nazmaris, preact, data son
trapo will be provider and to

ces and signatle bring tare pronu

Date:

Q. What are the concrete ways for IC members to catch AI manipulation and synthetic evidence in an inquiry?

As voice cloning and AI image generators become highly accessible, ICs are increasingly encountering weaponised synthetic media, such as fabricated chat screenshots or deepfake audio recordings. Because online AI detection software is not 100% reliable and yields false readings, the IC must implement a strict verification framework including a Digital Forensic Audit & Metadata Inspection which can be easily done by ICs can utilize tools like [jimpl Metadata Viewer](#) or [FotoForensics](#) to trace file history, with the express consent of the Data Principal. Since these carry the same risks as any other AI tool usage for confidentiality, the same can be done only with consent of parties. For images, Error Level Analysis (ELA) can highlight changes in pixel compression across an image. In a manipulated chat screenshot (e.g., WhatsApp, Slack, or Teams), text bubbles or elements inserted later will flash at a completely different brightness level under ELA compared to the rest of the file background.

Similarly, Spotting Audio, Visual Anomalies, Phoneme and Waveform Irregularities can be done for voice and video evidences. And most importantly, since technology alone cannot replace rigorous procedural inquiry, Live Data Export remains to be an effective way to check AI manipulation. IC can ask the complainant or respondent to open the active messaging application in front of the IC and export the chat history directly to an HTML or CSV file, eliminating reliance on easily doctored screenshots, as part of the inquiry.



How to view EXIF metadata from your photos

1

Upload a photo

Upload any [photo](#) to Jimpl EXIF Viewer. We'll read its metadata and show what's inside.

2

View the metadata

View EXIF metadata recorded in the photo. Date, time, [camera](#) settings, geolocation coordinates, and many more.

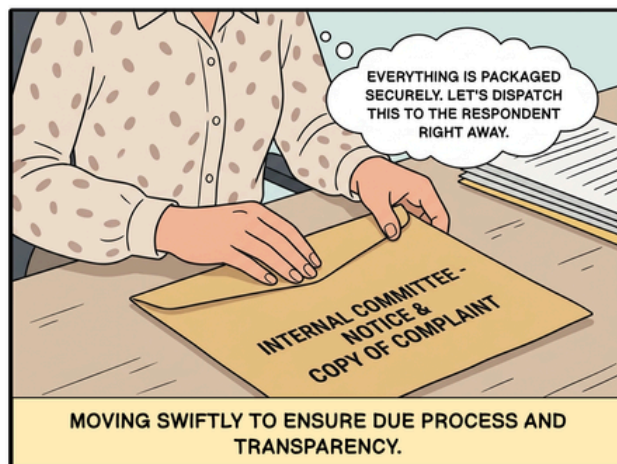
3

Remove the metadata

Download the photo with EXIF [data](#) removed. It's good to protect your privacy and reduce the photo file size.

How to view EXIF metadata on Jimpl.com

THE PROTOCOL IN ACTION



Internal Committee (IC): Send the complaint with enclosures to the respondent within 7 working days of receiving the complaint.

Respondent: Submit a written reply, supporting documents, and witness list with names and addresses within 10 working days of receiving the complaint.

Legal reference: Rule 7(2) and Rule 7(3), POSH Rules, 2013.

Ask the Legal Expert!

YOUR LEGAL QUERIES, ADDRESSED WITH
EXPERT INSIGHT.

1. Can an IC Seize an Employee's Personal Mobile Phone to Inspect WhatsApp Chats?

No. Section 11 of the POSH Act gives the IC specified civil court powers to seek documents, not powers to seize a personal phone. Refusing blanket access alone should not count against the person. Before drawing an adverse inference, the IC should consider the request's legality, relevance and scope, the person's control over the evidence, other ways to obtain it and their explanation, and record its reasons.

2. Does Sharing CCTV Footage with the Respondent Necessarily Breach Other Employees' Privacy?

No. Necessary disclosure for a fair inquiry is not automatically a privacy breach because others appear in the footage. Limit access and circulation, consider masking irrelevant identities or controlled viewing, and preserve adequate context and access for a meaningful defence.

3. Is Employee Consent Always Required to Review Corporate Email or Slack Records?

Not necessarily. Assess the purpose and scope under Section 7(i), and whether a necessity-based Section 17 exemption applies to the inquiry processing. Document the basis and use focused search parameters. Ownership of the system alone does not authorise unrestricted access.

4. Does Section 17 Shield Every Inquiry Activity from a DPDP Complaint?

No. The exemption depends on the processing meeting its statutory conditions and covers only specified provisions. Accountability under Section 8(1) and reasonable security safeguards under Section 8(5) remain where Section 17(1) applies. Unrelated processing, unnecessary disclosure or insecure handling cannot be treated as automatically protected; POSH obligations apply separately.

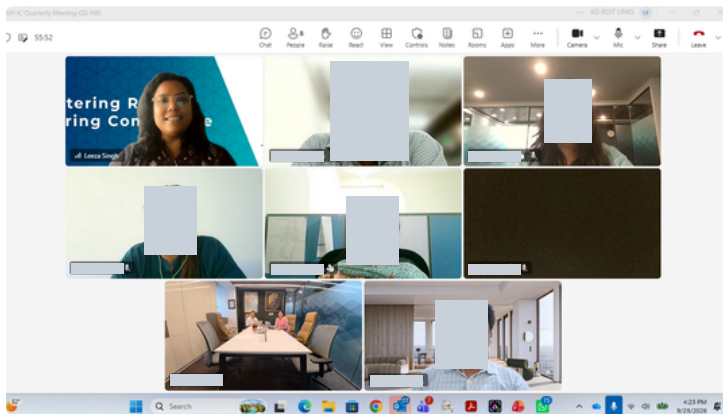
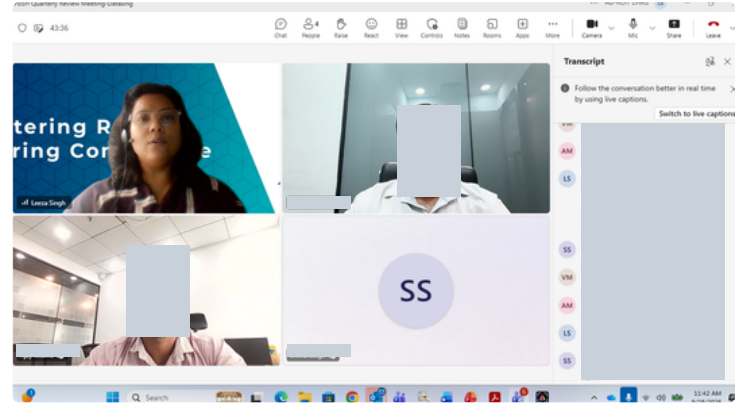
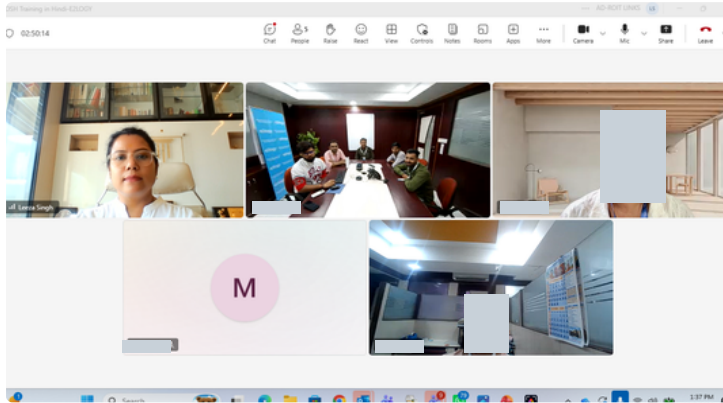
5. May Parties Record Virtual IC Hearings on Personal Devices?

The IC should establish clear recording arrangements and ordinarily prohibit unauthorised personal recordings and onward circulation. Section 16 does not expressly make every act of recording unlawful. Any permission, restriction or protective arrangement should consider confidentiality, fair procedure, applicable service rules and the specific circumstances.

6. How Long Should Digital Inquiry Records Be Retained?

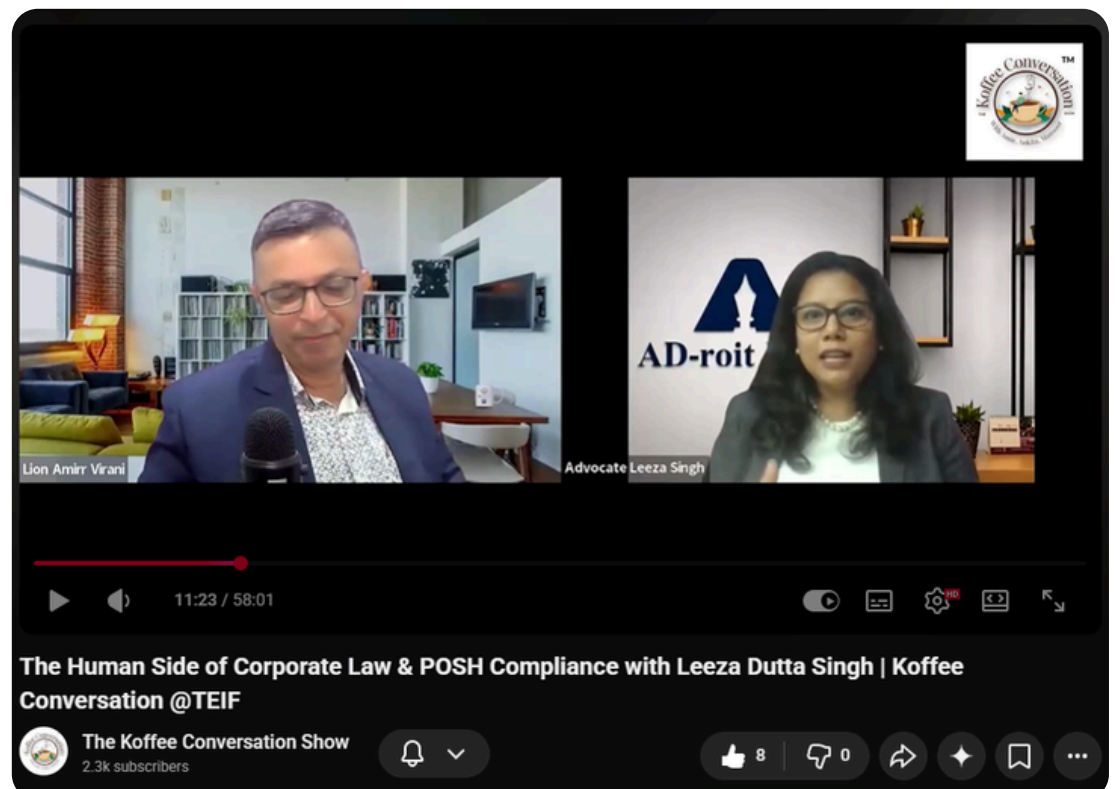
There is no universal POSH rule requiring deletion after ninety days. Preserve records for the inquiry, appeal rights, applicable legal or service-rule requirements and litigation needs. Review a documented retention schedule, release legal holds only when justified, and securely dispose of records once their lawful retention needs end.

Highlights in Frames



Online PoSH Trainings
with e2logy,
Nippon Koei India,
& Dataxing

Checkout the
Podcast at
[The Koffee
Conversation
Show](#)



Our Services



PoSH Compliance Training & Advisory

Building safer workplaces, one session at a time.



Diversity, Equity & Inclusion (DEI)

Creating cultures where everyone feels a sense of belonging.



Ethics and Code of Business Conduct

Empowering decisions with ethics and integrity.



Simplifying Labour Law Compliance

Turning complex laws into crystal clear solutions.



POCSO Awareness & Support

Protecting children through awareness and action.



Policy Drafting & Review

Policies that work — for people and compliance.



+91 96500-24706



leeza.singh@adroitlinks.com



@adroitlinks



adroitlinks.com



TS -29, 7th Floor, Hope Tower,
Galaxy Blue Sapphire Plaza, Plot
No. C-03, Sector-4, Greater
Noida (W), UP-201009