(1-62)

IN THE SUPREME COURT OF INDIA

CRIMINAL APPELLATE JURISDICTION

CRIMINAL APPEAL NO.1255 OF 1999

In the matter of:

Peoples Union for Civil Liberties and Anr. ...Petitioners

Versus

The State of Maharashtra and Ors. ...Respondents

POLICE MANUAL FOR MEDIA BRIEFING

ON BEHALF OF SR. ADV. GOPAL SANKARANARAYANAN, AMICUS CURIAE

FOR INDEX, KINDLY SEE INSIDE

ADVOCATE FOR THE AMICUS CURIAE: SHIVANI VIJ

INDEX

Filed By:

Shivani Vij
Advocate-on-Record, For the Amicus
G-12, Basement, Jangpura Extension, New Delhi-110048; +91 9630339000

Filed on: 08.11.2025

People's Union for Civil Liberties & Anr. vs State of Maharashtra and Ors.

POLICE MANUAL FOR MEDIA BRIEFING

GOPAL SANKARANARAYANAN
[AMICUS CURIAE]

TABLE OF CONTENTS

POLICE MANUAL FOR MEDIA BRIEFING

PART I — FOUNDATION, SCOPE AND PURPOSE

CHAPTER 1. PURPOSE AND GUIDING PRINCIPLES

1.1 Purpose

This Manual establishes a principled, rights-compatible, and investigation-safe framework for communications between the police and the public, as well as with the media. It aligns with the public's legitimate interest in timely, accurate information with:

- The dignity, privacy, and fair-trial rights of victims, witnesses, and suspects; and
- The integrity of police operations and criminal investigations.

Police communicate to prevent harm, correct rumours, enlist public cooperation, and maintain law and order. It is also extremely vital in the current social media age that the Police communicate only correct, verified, and necessary information to the public to prevent the spread of incorrect information, which has the propensity to disrupt law and order.

1.2 Scope and Applicability

This Manual applies to all the police personnel who collect, approve, or disseminate information externally, including dedicated spokespersons, District/Commissionerate media cells, on-scene information officers, social-media handlers, and any officer who addresses the media or issues public advisories, if need be. It covers all external communications: press notes, briefings, interviews, social-media posts, SMS alerts, public notices, posters, and audio-visual content.

1.3 Guiding Functions of Police Communication

Police communications serve 3 core functions:

- **Public Safety.** Timely advisories, helpline information, traffic/crowd instructions, missing-person and absconding suspects alerts, and threat mitigation guidance.
- **Transparency and Accountability.** Quick and effective dissemination of information, communicating process milestones (not case theories), recording due-process steps, and enabling informed public scrutiny.
- **Trust Building.** Neutral, victim-centric language; avoiding sensationalism, politicisation, or communalisation; modelling legality and restraint.

1.4 Disclosure Tests (All Must Pass)

Every media briefing shall satisfy all 4 tests below. If any test fails, bring the information into conformity with the tests:

- **Legality.** There is a clear legal/official basis to share; there is no statutory bar or court order that prohibits disclosure.
- **Necessity.** A concrete public-interest objective (safety, correction of harmful rumour, call for cooperation, maintenance of law and order) cannot be reasonably achieved without disclosure.
- **Proportionality.** Content is narrowly tailored: disclose only what is strictly necessary; minimise privacy breaches/violations and prejudice; apply redactions or share information that provides a broad idea.
- **Accountability.** Content is vetted and approved by the concerned police department regarding its veracity and delivered exclusively through the designated briefing cells.

1.5 Investigation Integrity and Fair Trial

To prevent prejudice and contamination of evidence:

- **Do not** comment on the merits of a case, disclose evidentiary theories, publish alleged confessions, or quote witness accounts.
- **Do not** disclose details that could taint identification parades, influence testimony, or pressure judicial processes.
- **Do** use neutral language and **holding statements** that report process milestones (e.g., "FIR registered," "search conducted," "suspects arrested/produced," "investigation ongoing") without implying guilt.
- **Do** protect the chain-of-custody and operational security: withhold investigative techniques, surveillance methods, and deployment details.
- **Do** correct misinformation spread by media houses or the public even after media briefings.

1.6 Survivor- and Victim-Centred Communication

To avoid re-victimisation and secondary harm:

- **Identity protection.** Withhold names, faces, voices, and **re-identifying details** (family relations, exact address, workplace/school, distinctive descriptors) unless lawfully obtained, informed consent covers that disclosure **and** release is demonstrably in the survivor's best interests.
- **Language.** Use trauma-informed, non-judgmental wording; avoid moralising, victim-blaming, or sensational detail.
- **Imagery.** Avoid images or audio that reveal identity or depict suffering; use generic visuals where necessary for public interest.

1.7 Non-Discrimination and Anti-Stereotyping

Do not reference caste, religion, ethnicity, disability, sexual orientation, gender identity, occupation, or migration status **unless strictly necessary** for immediate safety (e.g., suspects absconding). Avoid terms that stigmatise; prefer precise, neutral descriptors.

1.8 Rumours, Disinformation, and Online Virality

When misinformation threatens public order or fairness:

- **Assess.** Prioritise high-reach false narratives over one-off replies.
- **Respond with "Myth–Fact" cards** that (a) state the verified fact, (b) briefly identify the rumour without amplifying it, and (c) point to official channels for updates.
- **Escalate** to platform reporting where content incites violence, risks the dissemination of personal information of victims/witnesses, or violates court restrictions.
- **Record**s. Complete records, starting from the collection of information to dissemination, must be maintained by the Media Briefing Cells.

1.9 Accessibility and Language Standards

- Issue key releases in the dominant local language(s) and English. Use plain-language headlines.
- Caption all videos; provide alternate text for images.
- For emergency advisories, use simple bulletins and standard icons; include helplines and validity periods.

1.10 Authorisation and Ownership

Only designated spokespersons or officers authorised by the Head of District/Commissionerate/Unit shall brief the media or issue public statements. The Media Briefing Cell (MBC) is to maintain the calendar of briefings, the approval chain, and the official archive of all public communications.

1.11 Mandatory Records

Maintain a **Media Briefing Register** (physical or digital) capturing: date/time, channel, subject, approving officer, final text/asset, and links.

Retain drafts, approvals, and final artefacts in the official archive for audit and training.

CHAPTER 2. SCOPE AND APPLICABILITY

2.1 Organisational Coverage

As stated above, the manual shall apply to all tiers of policing within the State or Union Territory, including:

- **State Police Headquarters and Commissionerate**
- **Ranges/Zonal offices and**
- **District Police Offices**
- **Specialised units** such as Crime Branch, Cyber Crime, Anti-Terrorism Squad/Counter-Terrorism, Special Operations Group, Railway and Traffic Police, Women and Child Safety Units, Economic Offences Wing, Disaster Management Cells, and Police Training Academies.

Coordination with central investigative or enforcement agencies shall take place **only through the Media Briefing Cell (MBC)** to ensure unified, fact-consistent public communication.

2.2 Material Coverage

The Manual governs all forms of **external communication**, including:

- Press notes, press releases, and media statements;
- In-person or virtual press briefings and interviews;
- Replies to media queries and background clarifications;
- Official social-media posts on platforms such as X, Facebook, Instagram, or YouTube;
- Release of photographs, CCTV footage, or video/audio clips;
- Real-time updates during emergency, law-and-order situations, or disasters.
- Post-verdict update and public-order advisories and community-safety alerts.

2.3 Geographic and Jurisdictional Coordination

When multiple jurisdictions overlap:

- The **senior-most competent authority by incident type** (e.g., Commissioner/Joint Commissioner for Commissionerates, District SP for District Offices) shall lead all public communications.
- For events spanning multiple districts or States, the **State Headquarters MBC** shall coordinate and issue a single, consolidated release as the **"point of truth."**
- MBCs in Commissionerates and Districts shall **reproduce or amplify** the authorised content **without modification**, ensuring uniformity across jurisdictions.

2.4 Exceptions and Emergency Overrides

In exceptional or rapidly evolving situations such as terror incidents, communal tension, natural disasters, or mass-casualty events —

- The **Director General of Police (DGP)**, **Commissioner of Police (CP)**, or a **formally designated delegate** may temporarily:
    - Centralise all communications through the State Headquarters MBC.
    - Suspend decentralised briefings or briefings from lower levels.
    - Impose **time-bound embargoes** on field-level statements to prevent confusion.

2.5 Implementation Roadmap — 90-Day Adoption Plan

Timeline	Milestones	Key Outputs
Day 0 –30	Establish institutional infrastructure	Constitute and notify MBCs; designate authorised spokespersons; register and verify all official social-media handles; issue standard templates, holding statements, and branding guidelines.
Day 31 – 60	Capacity building	Conduct structured training for spokespersons, staff in MBCs, and Inspector/Sub-Inspector who are the first responders; simulate a mock press briefing; operationalise the media-logging and digital archive system.
Day 61 – 90	Validation and audit	Execute two live drills (crime-scene briefing and public-assembly management); publish a monthly compliance dashboard; complete a legal-vetting review of all templates and disclaimers.

CHAPTER 3. LEGAL AND POLICY FRAMEWORK

3.1 Constitutional Principles

Police communications operate within the guarantees and limits of the Constitution.

- **Article 19(1)(a)** recognises the public's right to receive information.
- **Article 19(2)** permits reasonable restrictions in the interests of public order, decency, defamation, and contempt of court.
- **Article 21** safeguards dignity, privacy, and personal liberty.

Accordingly, all public statements must be demonstrably tailored to these boundaries. Communications shall **not create or contribute to "trial by media."** Every disclosure should balance openness with fairness, privacy, and the presumption of innocence.

3.2 Criminal Procedure and Evidence Interface

Under the provisions of Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Adhiniyam (BSA):

- Case diaries, witness statements, confessions, and identification-parade details are legally protected materials.
- Public commentary on such evidence risks contaminating testimony and compromising admissibility.

Police officers shall therefore **restrict all briefings** to verifiable procedural milestones (e.g., FIR registered, suspects arrested, investigation continuing) and **avoid evidentiary details or speculative narratives.**

3.3 Special Laws Protecting Identity and Dignity

The following laws mandate strict confidentiality of identity:

- **POCSO Act, 2012 —** prohibits disclosure of names, images, addresses, or other identifying particulars of child survivors or victims of sexual offences.
- **Juvenile Justice (Care and Protection of Children) Act, 2015** — protects the identity of children in conflict with law or as witnesses/victims.
- **Indian Penal Code/Bharatiya Nyaya Sanhita provisions** on obscenity, defamation, and outrage of modesty reinforce these protections.

No police release shall include names, relational descriptors, locality details, or any **"Jigsaw Identifiers" (Information that has the probability of reaching to a conclusion of identification.)**
All visual material (CCTV, stills, clips) must undergo a **pre-release audit** to ensure zero inadvertent victim exposure.

3.4 RTI Interface and Proactive Disclosure

- Once a press release or advisory is officially issued, it shall be **proactively uploaded** to the police website and official social media handles. On the website, a dedicated section dealing with MBCs is to be updated.
- Information concerning ongoing investigations may attract the **exemption under Section 8(1)(h) of the RTI Act, 2005**—to prevent impediment to investigation or prosecution.
- This exemption must be **invoked narrowly, time-bound, and with written reasons recorded** in the MBC log.
- Denial of information does not preclude the release of generic process updates through holding statements.

3.5 Official Secrets, Security, and Operations

- Communications shall not disclose information that could compromise ongoing or future operations, tactical methods, surveillance, or intelligence sources.
- When public safety demands a warning (e.g., lookout for an armed suspect or terror threat), the content shall be limited to **essential safety details**, avoiding exposure of sensitive methods or capacities.

3.6 Data Protection and Platform Governance

- All official handles are custodians of **personal data** belonging to complainants, victims, and bystanders.
- Posts shall **avoid unnecessary personal information** unless disclosure serves a direct safety purpose.
- Access to digital platforms must be **role-based**, with mandatory password rotation, multi-factor authentication, and prompt revocation upon transfer or retirement.
- All takedowns or content edits shall be **logged with a timestamp and reason.**

3.7 Institutional and Industry Norms

Police spokespersons shall be guided by:

- **Press Council of India Norms of Journalistic Conduct (2022)**, and
- **News Broadcasting and Digital Standards Authority (NBDSA) Guidelines**,

Both of which prohibit sensationalism, speculative reporting, and publication of survivor or juvenile identities.

→ Neutral-language templates in this Manual are aligned with these standards.

3.8 Terminology Cross-Walk (Legacy to Current Codes)

Legacy Statute	Current Code/Equivalent	Relevance to Communications
Indian Penal Code (IPC)	Bharatiya Nyaya Sanhita (BNS)	Substantive offences and terminology
Code of Criminal Procedure (CrPC)	Bharatiya Nagarik Suraksha Sanhita (BNSS)	Procedural stages and investigation terms
Indian Evidence Act	Bharatiya Sakshya Adhiniyam (BSA)	Evidentiary admissibility and testimonial safeguards
Juvenile Justice Act	Unchanged (2015)	Identity-protection provisions
POCSO Act	Unchanged (2012)	Non-disclosure of survivor/child identity

Officers must read legacy references in older templates **mutatis mutandis** to the current codes.

3.9 Fair-Trial and Sub-Judice Safeguards

- Courts may issue **postponement or reporting-restriction orders** under Article 19(2) or contempt jurisdiction.
- The MBC shall **pre-brief spokespersons** on any such order and ensure statements remain within permitted limits. All such directions and compliance measures shall be **documented in the MBC register.**

- During active trials, only **holding statements** describing procedural progress shall be used.

CHAPTER 4. DEFINITIONS AND INTERPRETIVE NOTES

4.1 Key Terms

Term	Meaning/Definition
Press Release / Press Note	An officially approved, written communication containing verified facts and neutral language, issued for public dissemination and archived by the MBC.
Briefing / Press Conference	A scheduled on-record interaction with accredited media, led by a designated spokesperson, and supported by a written press note.
On-Record / Background / Embargoed	Attribution regimes: "on-record" is attributable by name; "background" conveys verified context without direct attribution; "embargoed" means non-publication until a stated time.
Identity / Identifier	Any data point (name, face, address, school, employer, family relation, vehicle number, or unique event descriptor) capable of directly or indirectly revealing a person's identity.
Personal Data / Sensitive Data	Personal data relates to an identifiable person; sensitive data includes health, sexual life, biometric, and child-related information.
Crime Scene	Any area under police control for evidence preservation and public safety; media access is restricted to the designated **Staging Area.**

Term	Meaning/Definition
Media Staging Area	A demarcated external zone where authorised briefings occur, maintaining distance from the evidence cordon while enabling visual access.
Pool Access	A controlled arrangement allowing one accredited crew to film or photograph for collective media use, ensuring minimal disruption.
Child	Any person under 18 years of age, whether victim, witness, or child in conflict with law.

4.2 Interpretive Notes

- Where legacy references (IPC/CrPC/Evidence Act) remain in existing circulars or templates, they shall be **read in line with** the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA).
- In the event of conflict, **statutory provisions, court directions, and the updated Manual** shall prevail, in that order.
- Periodic legal reviews shall update templates and references accordingly.

4.3 Risk-Assessment Matrix (Indicative)

Before every disclosure, the MBC shall rate each parameter below as **Low / Medium / High** and record it in the log. Disclosures with **unacceptable cumulative risk** shall be deferred, anonymised, or replaced with a holding statement.

Parameter	Description
1. Public-Interest Necessity	Is there a pressing safety or transparency objective?
2. Prejudice to Fair Trial	Could this disclosure influence witnesses, jurors, or judicial perception?
3. Privacy / Identification Risk	Could it directly or indirectly identify victims, survivors, or minors?
4. Operational / Security Risk	Does it expose tactics, personnel, or future operations?
5. Rumour-Suppression Value	Will it help quell misinformation or panic?
6. Impact on Survivors / Juveniles	Could it retraumatise or stigmatise affected persons?

4.4 Language Standards — Do's and Don'ts

Do	Don't
Use neutral verbs: "stated," "said," "clarified."	Avoid speculative or judgmental verbs: "confessed," "admitted," "claimed."

Do	Don't
Mention factual details: date, time, sections invoked, next procedural step.	Avoid discussing evidence, confessions, or witness statements.
Use plain, descriptive language.	Avoid adjectives implying moral judgment ("heinous," "bogus," "brutal").
Attribute information to the institution, not the individual officer.	Avoid personal opinions, forecasts, or moral commentary.
Verify all facts before release.	Never release unverified or third-party information.

PART II — AUTHORITY, STRUCTURE AND WORKFLOW

CHAPTER 5. AUTHORITY TO COMMUNICATE — DESIGNATION, DELEGATION AND OVERRIDES

Purpose: To establish which Police officer may speak to the media about an incident, under what authority, and through which channels.

5.1 Designation Orders (Who May Speak)

- Each State Headquarters, Commissionerate, Range, District, and Specialised Unit shall, by written order, designate one **Spokesperson (SPOX)** and two alternates.
- The designation order shall specify: name, rank, tenure, jurisdictional or subject-matter scope, and authorised channels (press notes, on-record briefings, official social-media accounts).
- Case Investigating Officers (IOs) and staff shall not issue quotable statements or share case-specific information directly with the media. All external communications shall flow through the Media Briefing Cell (MBC) and be attributed only to the SPOX.
- Designations shall be reviewed quarterly and upon transfer or long leave of the incumbent. The current designation list shall be displayed on the police website and internal dashboard.
- The SPOX shall maintain a shadow file containing copies of all media releases and statements issued under its name.

5.2 Delegation Matrix

Communication Action	**Responsible**	**Accountable**	**Consulted**	**Informed**
Draft press note	MBC Content Lead	SPOX	IO, Legal Vetting Officer, Prosecution Officers	SP/SSP/IG
Approve talking points	SPOX	Senior most officer in the relevant hierarchy.	IO, Legal Vetting Officer, Prosecution Officers	SP/SSP/IG
Social-media post (official account)	MBC	SPOX	Legal Vetting Officer (for sensitive content)	Senior most officer in the relevant hierarchy.
Emergency corrections or rejoinders	MBC	SPOX	Legal Vetting Officer	Senior most officer in the relevant hierarchy.

5.3 Emergency Overrides

- During rapidly evolving incidents (terror threats, major public-order events, mass casualty situations), the DGP/CP or authorised delegate may temporarily **centralise messaging.**
- A written override memo (email or SMS-backed) shall record the start time, scope of topics and channels affected, and approving authority.
- The override period shall not exceed **48 hours** unless formally renewed.
- The override and all statements issued thereunder shall be archived and reviewed post-incident by the MBC.
- MBCs at all levels shall echo the single "source of truth" to avoid contradictory narratives.

  Outcome: Centralised and coherent information flow during emergencies.

5.4 Multi-Jurisdiction and Inter-Agency Coordination

- When incidents span multiple districts or States, the senior-most jurisdiction by incident type shall lead communications. State HQ MBC coordinates language localisation and uniform dissemination.
- Where central agencies are involved, the State HQ shall appoint a nodal officer for unified messaging. All content is cleared through that office to ensure legal and operational discipline.
- In cross-border operations or arrests, the home State SPOX shall issue neutral process updates and defer evidentiary comment to the lead agency.
- Joint press notes shall carry only the lead State HQ MBC contact in the footer for consistent attribution.

5.5 Legal Basis for Authority

- Authority to communicate derives from the State Police Act, relevant provisions of the Police Manual, standing orders, and specific designation orders issued thereunder.
- Unauthorised interviews, leaks, or disclosures are violations of the present manual and shall be treated as misconduct with necessary proceedings under the State Police (Conduct) Rules to be initiated.
- Such violations shall trigger disciplinary proceedings and, where necessary, prosecution for breach of official secrecy or contempt of court. **Outcome:** Legal accountability is embedded in communication authority.

CHAPTER 6. MEDIA BRIEFING CELL (MBC) — STRUCTURE, STAFFING AND WORKFLOWS

To define the institutional machinery that manages all external communications.

6.1 Organisational Structure

- Each jurisdiction [Ref 2.1] shall maintain a Media Briefing Cell (MBC) as the **single nodal interface** for press releases, briefings, social-media content, and media credentials.
- Minimum staffing pattern: (i) Public Relations Officer / PIO (Lead); (ii) Legal Vetting Officer; (iii) Digital Content Lead; (iv) Archival & Analytics Officer; (v) Digital Communications Officer (DCO) for official handles; (vi) On-scene PIO roster.
- Each MBC shall report functionally to the SPOX and administratively to the CP/SP/DGP as applicable.

6.2 24/7 Roster and Escalation

- A weekly roster shall list on-duty personnel, alternate contacts, and escalation hierarchy, shared internally and with accredited media.
- Service Level Agreements (SLAs): (a) holding statement within 30–60 minutes of a major incident; (b) first press note within 2–4 hours after legal vetting; (c) scheduled updates thereafter.
- If the 30-minute SLA cannot be met, an interim statement shall be issued acknowledging the incident and committing to updates.
- Unacknowledged queries escalate to the SPOX, then to the CP/DGP Secretariat if time-critical.

6.3 Workflow (Intake → Draft → Vet → Approve → Publish → Archive)

- **Intake:** IO or first responder submits a facts-only incident sheet (time, place, sections, milestones, advisories).
- **Draft:** Content Lead prepares a neutral-language press note, podium talking points, and Q&A binder with approved "No Comment" responses.
- **Vet:** Legal Vetting Officer screens for privacy, identity, sub judice constraints, and operational sensitivity.
- **Approve:** SPOX signs off; sensitive cases require CP/DGP or delegate approval.
- **Publish:** DCO posts to official handles; MBC emails PDF press note with unique ID; uploads to website with alt text, captions, and bilingual headline.
- **Archive:** Archive Officer logs version, timestamp, distribution list, and attachments; stores recordings and issue-tracker entries for corrections and rejoinders.

6.4 Tools:

a) **Templates:** press note; holding statement; Q&A binder; media list; incident log; rejoinder notice; postponement-order compliance note.
b) **Registers:** designation orders register; social-handle registry; media credentials register; takedown log; monthly compliance dashboard.
c) **Systems:** ticketing software for media queries; restricted shared drives; password vault with multi-factor authentication; immutable digital archive with audit trails.
Outcome: Institutional memory and compliance are ready for inspection or RTI audit.

6.5 Legal Vetting Checklist (Indicative)

☐ Identity and identifiers removed (survivors/juveniles; jigsaw risks).

☐ No evidentiary theories, confessions, or witness accounts.

☐ Neutral phrasing; no adjectives signalling guilt or innocence.

☐ RTI S. 8(1)(h) invoked if ongoing investigation details withheld.

☐ Sub judice and postponement-order compliance checked.

☐ Operational sensitivities screened (sources, methods, tactics masked).

☐ Platform and accessibility standards met (alt text, captions).

☐ Data-protection principles observed (minimal personal data, lawful basis, retention tags).

6.6 Accreditation and Access

- Maintain a media-accreditation register with verified organisation details and contact numbers.
- Misuse or safety violations may lead to temporary suspension after notice. An appeal lies to the DGP within 30 days.
- In respect of crime scene briefings- The on-scene PIO shall issue periodic factual updates and safety instructions from the staging area.

6.7 Capacity Building

- Annual certification is mandatory for SPOX, IOs, and DCOs covering: neutral language, trauma-informed communication, sub judice law, contempt and defamation, accessibility, data protection, and misinformation response.
- Police Training Academies shall integrate MBC modules into induction and in-service courses.
- Certification status shall be recorded in the officer's service book and required for re-designation as SPOX or DCO.

CHAPTER 7. DOCUMENTATION, RECORD-KEEPING AND AUDIT TRAILS

7.1 Mandatory Logs

- For every press release or briefing, the MBC shall maintain a log containing: a unique identification number; date and time; case or event reference; stage of proceedings; authorising officer; channels used; media present; hyperlinks to uploads; file hashes of PDFs or videos; and public-contact details for cooperation or leads.
- All entries form part of the permanent audit record and must be updated contemporaneously.

7.2 Archival Standards and Retention

- Press notes shall be archived as digitally signed PDF files. Raw artefacts, including recordings of pressers, social-media posts, and Q&A transcripts, remain linked to the same unique ID.
- Retention standards: minimum three years for routine briefings; seven to ten years for serious offences or public-order incidents; longer where litigation is pending or foreseeable.

- Legal holds shall be recorded wherever a court or inquiry requires extended preservation.
- Corrections, rejoinders, and takedown histories are attached to the original record to maintain full context.

7.3 Corrections, Rejoinders and Legal Responses

- Each MBC shall operate a monitoring and corrections tracker. Where factual errors or misreporting are identified, a neutral rejoinder is issued stating verified facts, linking to the original release, and avoiding any attribution of motive.
- Legal notices are used only when demonstrably necessary to address harmful misinformation; transparent correction remains the preferred approach.
- A monthly communications scoreboard summarises: number of releases and briefings, corrections issued, sub judice events, RTI 8(1)(h) invocations, takedowns, training completions, and disciplinary actions (category-wise).

7.4 Accountability and Discipline

- Good-faith mistakes lead to coaching and process improvement. Deliberate leaks, unauthorised statements, or political messaging attract proportionate disciplinary action under the relevant service-conduct rules.
- Repeat non-compliance escalates penalties and may result in removal from communication duties.
- A register of infractions is maintained linking each case to remedial training or disciplinary outcome for institutional learning.

7.5 Transparency and Proactive Disclosure

- All press releases, advisories, and presser videos shall be posted on official websites and verified social-media handles with a disclaimer that only MBC-issued information is authoritative
- Designation orders and current SPOX/MBC rosters shall be published for clarity to the media and public.

CHAPTER 8. STAGE-WISE DISCLOSURE PROTOCOLS

8.1 Pre-FIR / Intake (Verification and Safety)

- **Purpose**: Prevent panic, invite verifiable tips, and issue safety advisories without identifying individuals or prejudging allegations.
- **Disclose**: General description of incident type, verified time window, broad locality (avoid micro-identifiers), safety steps, and one contact channel for leads.
- **Withhold**: Names, addresses, images, complainant or witness details, motive or modus theories, and any description that could enable jigsaw identification.
- If social-media rumours **escalate**, issue a neutral holding statement with helplines. If multiple false versions circulate, release a myth–fact card linking to the holding note.

8.2 FIR Registration

- **Disclose**: Offence sections, date and time, police station, broad location, IO designation, single contact point, and any safety advisory.
- **Withhold**: Complainant identity, witness names, sensitive circumstances, narrative of allegations, or any description identifying survivors or juveniles.
- **Checklist:** sections invoked; time–place basics; neutral wording; no adjectives; disclaimer that investigation is underway; upload signed PDF press note with unique ID.

8.3 Investigation (Ongoing)

- **Disclose**: Verified updates required for public safety or to seek assistance (for example, helplines or advisories concerning a suspect absconding designed to avoid over-identification).
- **Withhold**: Evidence theories, confessions, witness accounts, forensic details, CDR or CCTV snippets, and investigative tactics.
- **Risk flags**: high-profile matters, communal or caste sensitivities, minors, sexual offences, custodial contexts, data breaches, cross-border or terror elements.

- If an update is not essential for safety or crowd management, prefer silence and refer to the holding note. Where disclosure is essential, use redacted descriptors and time-boxed updates.

8.4 Arrest / Remand — Due Process, Not Spectacle

- **Disclose**: Arrest confirmation, date and time, legal sections, broad location, and due-process steps such as medical examination and production before the court.
- **Withhold**: Mugshots, walk-through visuals, travel itineraries, confession claims, witness mentions, or identifiers of protected persons.
- **Operational note**: Never parade the suspects. Mask faces where unavoidable visuals arise, and avoid adjectives implying guilt or motive.

8.5 Chargesheet / Framing of Charges — Procedural Milestones Only

- **Disclose**: Filing of final report, statutory sections, court name, next procedural step, and contact for victim services if relevant.
- **Withhold**: Case diary content, witness lists, TIP details, forensic or digital evidence, and any narrative of alleged acts beyond what is in the public domain by court record.
- **Checklist**: procedural facts; no evidentiary commentary; sub judice disclaimer; archive PDF with unique ID; Q&A confined to procedural posture.

8.6 Trial / Sub Judice Phase — Court-First Discipline

- **Disclose**: Scheduling information and public-interest advisories where necessary (for instance, traffic or assembly management around court premises).
- **Withhold**: All comments on merits, witnesses, credibility, confessions, or evidentiary strength. Refrain from selective leaks or narrative framing.

8.7 Post-Conviction / Post-Acquittal — Factual Outcome, Neutral Tone

- **Disclose**: Outcome of trial, sentencing details, or appellate stance if institutionally cleared.

- **Withhold**: Victim or witness identifiers, opinions on the court's reasoning, or details likely to trigger public-order risks unless safety advisories are essential.
- When **sensitivity or volatility** exists, centralise messaging at State HQ, timestamp all updates, and coordinate with District Administration for crowd-management advisories.

CHAPTER 9. MEDIA ACCESS AT INCIDENTS — SCENE INTEGRITY AND REASONABLE ACCESS

9.1 Perimeters and Staging

- Establish inner perimeters for investigators and outer perimeters for the public and media. Identify a safe staging area outside the evidence cone but within sight of the scene. Use signage and brief designated media marshals.
- Where space or safety is constrained, permit one camera, one television reporter, one print reporter, and one photographer under a pool-access arrangement to share feeds. No live shots are permitted within police cordons.

9.2 Scene PIO Duties

- The on-scene Public Information Officer announces the time of the next updates, issues safety and traffic advisories, repeats helplines, discourages speculation, and reiterates the single source-of-truth handles.
- A timestamped log of every statement is maintained, and the corresponding press note is uploaded promptly.

9.3 Visuals and Recording

Filming of victims, juveniles, or children in conflict with the law is prohibited. Sensitive assets and undercover personnel must be masked. Drone or aerial overflights that could expose tactics or victims require explicit clearance.

9.4 Accreditation and Conduct

Only accredited media may enter the staging area. Identity cards are verified, and safety constraints are briefed. Access may be withdrawn for breaches that endanger safety, with a reason and appeal route recorded.

9.5 Evidence Protection and Contamination Avoidance

Media shall not handle objects, cross-trace paths, or use flash where it risks damaging forensic evidence. Camera lines are marked and coordinated with forensic teams for any visuals cleared for release.

CHAPTER 10. PROHIBITED AND RESTRICTED DISCLOSURES — REDACTION BY DESIGN

10.1 Absolute Prohibitions

- Identity or identifiers of survivors of sexual offences and all children (victims, witnesses, or children in conflict with the law).
- Case-diary contents, witness statements, identification-parade details, confessions, or raw CCTV and digital evidence.
- Operational specifics that compromise national security or ongoing operations.
- Statements likely to cause contempt of court or prejudice proceedings, including adjectives implying guilt or innocence.

10.2 Restricted Disclosures (Context-Bound)

- Identity of the suspects [eg: A sensitive matter that could lead to communal riots or law and order issues if the identity of the suspects is disclosed]
- Privacy-intrusive details such as medical information, family relations, schools, or residences.

- Exact locations in domestic-violence or stalking matters and timestamps that permit re-identification.
- Travel or movement logistics of suspects between police stations, hospitals, prisons, or courts.

10.3 Redaction Matrix

- Identifiers to remove include names, faces, addresses, institutions, family or professional relationships, micro-locations, and distinctive injuries or disabilities that are non-essential.
- Language controls require avoidance of adjectives such as *heinous* or *brutal*, substitution with neutral verbs, and use of procedural phrasing (e.g., "arrested under sections ...").
- Data minimisation requires disclosing only what is strictly necessary for the legitimate objective—public safety, verification, or cooperation—and recording the lawful basis and retention tag in the archive log.

10.4 Decision Tree — Can This Be Disclosed?

- **Step 1**: Is the purpose safety, verification, or public calm? If no, do not disclose.
- **Step 2**: Can the objective be met without identifying anyone? If yes, redact and proceed.
- **Step 3**: Will disclosure impede investigation or fair trial? If uncertain, escalate to the Legal Vetting Officer and defer.
- **Step 4**: Is there a court order, statutory bar, or policy prohibition? If yes, do not disclose; issue a holding statement instead.

CHAPTER 11. SENSITIVE CATEGORIES AND SPECIAL CIRCUMSTANCES

11.1 Sexual-Offence and POCSO Matters

- Maintain strict anonymity for survivors and children. Use survivor-centric language and share only consented information about victim-support services.
- Avoid granular details of time or location that enable re-identification. Coordinate with Child Welfare Committees and One-Stop Centres for referral and assistance messaging.
- CCTV/Videography Releases: When suspect visuals are published, ensure survivors are not visible; blur backgrounds where necessary.

11.2 Juveniles in Conflict with Law and Child Witnesses

Do not disclose any identifying details. Consult guardians before including non-identifying demographic references. The court alone determines if identity may be revealed later; police shall not pre-empt disclosure.

11.3 Domestic Violence, Stalking and Harassment

Suppress micro-locations, relational descriptors, and daily-routine clues that may expose survivors. Provide helplines and safe-contact options in every release instead of personal details.

11.4 Communal and Caste-Sensitive Incidents / Public Order

Use neutral, de-escalatory language. Avoid attributing motive or group labels until verification is complete. Centralise messaging at State HQ, issue multilingual updates, and release myth–fact cards with time-stamped corrections.

11.5 Terror, Insurgency and High-Risk Operations

Delay any detail that compromises tactics or safety. Coordinate with central agencies. Publish perimeters, advisories, and helplines; refrain from naming suspects until cleared by the lead agency.

11.6 Custodial Deaths and Alleged Excesses

Acknowledge the incident immediately. Initiate all mandated legal processes such as magisterial inquiry and statutory intimations. Appoint a family liaison officer. Share only procedural steps, avoiding speculation on cause or witness identity.

11.7 Suicides and Self-Harm

Do not publish method, location specifics, or images. Use non-sensational language and always include mental-health helplines. Remove any content that may trigger imitation or distress.

11.8 Missing Persons (Adults and Children)

Publish carefully worded suspect-absconding advisories. Obtain guardian or parental consent for minors. Avoid over-identification through detailed appearance or background information. Document the takedown protocol once the person is traced.

11.9 Cyber-Enabled Crimes and Data Breaches

Describe the nature or scope of the breach without revealing technical details that could aid offenders. Provide citizen-safety guidance and reporting channels. Commit to a public summary once the inquiry concludes, omitting evidentiary material.

11.10 Disaster and Mass-Casualty Events

Hold joint briefings with Disaster Management authorities. Publish helplines, shelters, and multilingual advisories. Use pooled feeds where feasible. Avoid publishing images that identify victims or show bodies without consent.

CHAPTER 12. SUB JUDICE AND FAIR-TRIAL SAFEGUARDS

12.1 Contempt and Prejudice Risks

Avoid statements on merits, witness credibility, confessions, or evidence strength. Do not imply investigative theories or outcomes. Maintain strict neutrality throughout the trial period.

12.2 Postponement Orders and Specific Court Directions

Before issuing any update in matters under court-imposed limits, brief internal teams on the exact order. Holding statements must mirror the language and scope of the restriction. Archive both the order and compliance notes with timestamps.

12.3 Templated 'No Comment' Binders

Prepare Q&A cards for predictable questions about motive, confessions, or witness numbers. Responses must provide legally grounded refusals that educate without confrontation.

12.4 Rebuttals and Rejoinders During Trial

Use neutral corrections that cite the authoritative press note or court record. Avoid attributing motive to media reporting. Log each correction with hyperlink and timestamp in the archive.

CHAPTER 13. MEDIA STAGING LOCATION

13.1 Site Selection and Layout

Select a site with safe entry and exit, minimal interference with operations, and reliable power and connectivity. Mark camera positions, provide a podium with audio support, and designate a media marshal to manage flow.

13.2 Access Rules and Schedules

Publish the timing of briefings in advance and maintain consistent update intervals. Make clear that unscheduled or informal briefings will not occur. Provide press kits immediately after each update.

13.3 Accessibility and Inclusion

All posted videos shall include captions; images carry alt-text; advisories use bilingual headlines and plain language. For sensitive matters, provide a quiet-zone option for interviews or smaller briefings.

13.4 Documentation and After-Action Learning

Record all spoken statements and archive video and audio. Conduct an after-action review focusing on timing, clarity, adherence to redaction standards, and any corrections issued. Feed observations into monthly compliance dashboards and future training.

PART III — HOW TO BRIEF

CHAPTER 14. PRESS RELEASE ESSENTIALS

A press release is the authoritative, citable document through which verified information is shared with the public by the Police Department through the media. It must communicate essential facts without prejudicing investigation or fair trial, & always carry a disclaimer-only MBC-issued content on official channels is authoritative.

14.1 Purpose and Scope

The press release communicates verified facts that the public is entitled to know. It must answer the basic questions — Who, What, When, Where, Why, and How — in neutral language and avoid speculation or opinion.

14.2 Anatomy of a Release (Structure)

- Header — Department name, seal, unit, date/time, unique release ID, and MBC contact.
- Headline — Factual and neutral; no adjectives implying guilt or innocence.
- Lead Paragraph — Verified essentials: statutory sections, time window, broad location, and immediate safety instructions.
- Body — Procedural posture (for example, FIR registered, IO assigned, chargesheet filed), appeals for information, and public-safety or cooperation messages.
- Boilerplate and Disclaimer — Statement of single source of truth, sub judice posture, accessibility note, and bilingual availability (English + State language).
- Footer — SPOX name, designation, signature, URL, and contact hours.

14.3 Content Inclusions and Exclusions

- **Include only**: statutory sections invoked; verified timeline; public-safety advisories; route diversions; standard helplines; and appeal contacts (phone/email/portal).
- **Exclude entirely**: complainant or witness identifiers; photographs of suspects; confession claims; detailed evidence or narrative accounts; or any material beyond what is required to seek cooperation or ensure safety.

14.4 Drafting Standard

- Use short, declarative sentences and procedural verbs such as *registered, produced before the court, and search conducted under warrant.*
- Avoid speculation about motive.
- Replace adjectives with verifiable facts & use person-first terms as *survivor* or *child.*
- Apply redaction prompts to remove names, addresses, or faces of protected persons, micro-locations, and distinctive injuries.
- Where essential, use approximate ranges ("evening hours") rather than precise timestamps.
- Ensure accessibility: alt-text for images, captions for videos, readable PDFs, bilingual headings, and large-type advisories.

14.5 Workflow and Approvals

- Follow the sequence — Intake → Draft → Legal Vet → SPOX Approval → Publish → Archive → Monitor.
- Maintain a time-stamped ticket for each action. Sensitive releases require CP/DGP clearance for talking points.

14.6 Versioning and Archival

- Retain the original DOCX, signed PDF, checksum, and upload link. Record all corrections with the previous and revised text, plus timestamps.

14.7 Distribution

Upload the signed release to the official website and verified social handles. Email the PDF to the accredited media list (BCC) and post a summary thread linking to the document. For sensitive or high-impact matters, mirror the release on the State HQ site.

14.8 Scenario-Specific Inserts (Specimen Language)

- Sexual Offences / POCSO — *"We will not share any identity or location details of survivors or children. Support services are available at [helplines]."*
- Public Order / Communal Sensitivity — *"Avoid speculation or sharing unverified content. Follow only official updates issued at [times/handles]."*
- Disaster / Mass Casualty — *"Helpline: [numbers]; Missing Persons Desk: [contact]; Traffic Diversions: [broad routes]."*
- Cyber-Enabled Crimes — *"Do not share screenshots of private data. Report via [portal]. Verified guidance will be published as available."*

14.9 Sample Press Release Template

[Header — State Police / Unit]

Press Note ID: PN-[Unit]-YYYYMMDD-[Seq]

Date/Time: ____

Headline: Neutral factual headline

Body: (1) Verified facts (2) Sections invoked (3) Procedural step (4) Safety advisory (5) Appeal for information (phone/email/portal with hours).

Boilerplate/Disclaimer: *"Only information issued by the Media Briefing Cell through official channels is authoritative. The matter is under investigation/sub judice; we cannot comment on evidence or witnesses."*

SPOX: [Name / Rank / Contact] **Signature:** ____

14.10 Metrics (Release Quality Dashboard)

Monitor: time-to-first-release; correction latency; number of redaction errors; accessibility compliance rate; bilingual coverage; media pickup versus misinformation incidents; and qualitative stakeholder feedback.

CHAPTER 15. PRESS CONFERENCE PROTOCOLS

15.1 Necessity Test

Hold a press conference only when required in the public interest—such as major safety advisories, disaster coordination, or clarification of serious misinformation. For routine updates, prefer written press notes.

15.2 Pre-Conference Checklist

- Prepare a decision memo stating the purpose, key messages, and risk assessment. Select a venue away from active scenes; ensure a security sweep and clear ingress and egress routes.
- Assemble a podium binder containing the opening statement, approved talking points, "no-comment" cards with legal basis, and myth–fact cards if required.
- Verify accreditation and plan pool access where space is constrained. Check AV setup—microphones, backup recorder, and power supply—and arrange a sign-language interpreter if feasible.
- Brief the on-scene PIO and media marshals; mark the staging area. If live-streaming is approved, pre-define safe camera angles and enable captions.

15.3 Conduct and Q&A Management

- Begin and conclude on time. Read the opening statement verbatim and announce a defined Q&A window.

- Prioritise safety and service-related questions. If queries drift into prohibited areas, pivot to approved language or use "no-comment" cards citing the legal ground (for example, sub judice, privacy).
- Avoid off-the-record discussions and maintain equal access for all media. Do not parade or display suspects or disclose protected identities.

15.4 Recording and Publication

Record the full audio-video using a primary and backup device. Publish the transcript and corresponding press note immediately afterwards. Upload the video with captions and host all materials on official websites and handles with unique IDs.

15.5 Safety, Crowd and Evidence Integrity

Demarcate perimeters, restrict filming inside inner cordons, and prohibit drone operations unless specifically cleared. Coordinate with forensic teams to prevent evidence contamination.

15.6 Roles and Run-of-Show

- Roles: SPOX (lead), Legal Vetting Officer, Digital/Content Lead, DCO (live-stream), Media Marshal(s), Archivist.
- Run-of-Show: (1) Arrival and accreditation (2) Opening statement (3–5 min) (3) Q&A (8–12 min) (4) Closing with next-update time (5) Press-kit distribution (6) Uploads and archival (7) After-action review.

15.7 Handling Hostile or Leading Questions

- Use bridging phrases such as "We will not discuss evidence while the matter is before the court...," "Our focus is public safety; verified facts are in today's press note...," or "Please refer to the myth–fact card uploaded with this release."
- Document persistent violations and consider restricting access for repeat offenders under the accreditation policy.

15.8 After-Action Review (AAR)

Within twenty-four hours, record lessons learned on message clarity, redaction compliance, timing, media behaviour, misinformation corrections, and public order impact. Feed findings into monthly compliance dashboards.

15.9 Specimens

Opening-statement template; Q&A "no-comment" cards (sub judice, privacy, juveniles, operational security); media-advisory template; and myth–fact card paired with Press Note ID.

CHAPTER 16. SOCIAL MEDIA GOVERNANCE

16.1 Governance Architecture

- All command-level accounts are supervised by the Digital Communications Officer (DCO) and registered in a central directory.
- Posts follow a workflow: draft → legal vet (when needed) → SPOX approval → posting by the DCO.
- Passwords and multi-factor authentication are centrally managed; access is strictly role-based and logged.

16.2 Content Standards

- Posts shall provide factual updates, safety advisories, and corrections or rejoinders when necessary.
- No political content, commentary on ongoing cases, or debate with individuals is permitted. Tone must remain courteous, neutral, and service-oriented.

16.3 Accessibility and Inclusion

Provide alt-text for images, captions for videos, and avoid text embedded in images without accompanying text. Use bilingual headlines and summaries when appropriate.

16.4 Moderation and Community Management

- For sensitive posts, disable or limit replies where platforms allow. Avoid one-to-one debates; route complaints to designated grievance channels.
- Log direct messages and tips as tickets, acknowledging receipt without promising outcomes.

16.5 Platform-Specific Guidance (Indicative)

- Short-text platforms (microblogs): Use threaded updates with a link to the press note; pin the authoritative thread.
- Image or video platforms: Avoid identifiable faces; blur where unavoidable; always caption.
- Video or live-stream services: Pre-approve scripts; disable comments if moderation is infeasible; archive the recording with captions.
- Messaging or broadcast channels: Share only signed PDFs and safety advisories; never forward third-party content or rumours.

16.6 Corrections, Takedowns and Rejoinders

- Prefer transparent corrections and dated rejoinders over silent deletions.
- When deletion is required—for privacy, court order, or statutory breach—capture a screenshot, record reason and timestamp, and archive before removal.
- If feasible, post an updated version with a clear correction note.

16.7 Security and Incident Response

- Enable multi-factor authentication; rotate passwords quarterly; revoke access immediately on transfer or retirement.

- Maintain a compromise-response playbook covering signal loss, phishing, and impersonation.
- If an account is compromised, issue an advisory from mirror channels, contact the platform, and publish a signed clarification once control is restored.

16.8 Data Protection and Retention

- Collect the minimum personal data necessary in comments or messages and redirect users to official reporting portals.
- Archive all posts, comments (exported where feasible), and takedown logs with unique IDs.
- Retention periods mirror those of press-note archives.

16.9 Executive and Personal Accounts

- Handles of senior officers acting in an official capacity follow the same governance and civility norms as institutional accounts.
- Personal accounts must not comment on ongoing cases or disclose privileged information.
- Officers are encouraged to include a short "personal views" disclaimer and maintain a clear separation of personal and official content.

16.10 Measurement and Reporting

The DCO compiles a monthly dashboard showing time-to-first-post, correction latency, accessibility compliance, misinformation incidents handled, helpline engagement metrics, language coverage, platform-security events, and closure rates.

PART IV — OPERATIONS, TRAINING, AND COMPLIANCE

CHAPTER 17. CRISIS COMMUNICATIONS

17.1 Using These Playbooks

Crisis communications are high-stakes moments that test both institutional discipline and public trust. This chapter provides playbooks for predictable emergency scenarios, ensuring consistency, legality, and composure under pressure.

Each playbook sets out:

(i) **Trigger conditions**;
(ii) **Immediate actions** during the first hour;
(iii) **Sustained updates** for the first 24 hours;
(iv) **Disclosures to include and withhold**;
(v) **Sample neutral language**;
(vi) **Roles and approvals**; and
(vii) **Metrics and exit criteria**.

All officers must adapt these steps to local context, applicable laws, and any court-imposed communication restrictions. The aim is to maintain factual accuracy, public calm, and fairness to all parties while safeguarding investigation integrity.

17.2 Common Tools

Standard artefacts used in crisis communication include:

- **Holding Statement** — a verified interim message confirming awareness of the event and promising updates.
- **Myth–Fact Card** — short, time-stamped clarifications countering specific falsehoods.

- **Media Advisory** — structured briefing notice specifying timing, format, and spokesperson.
- **Social Thread Template** — pre-approved bilingual update chain for verified information.
- **Map-Based Advisory** — route, perimeter, or shelter guidance using standard symbols.
- **Court-Restricted Line** — pre-drafted compliant language for matters under reporting restraint.
- **After-Action Review (AAR)** — structured debrief assessing performance and lessons learnt.
- Each communication carries a **unique ID, timestamp, approver signature, and archival record**, ensuring accountability and traceability.

A. Major Communal Tension Incident

- **Trigger:** Communal or caste-sensitive flashpoints with misinformation or violence risk.
- **Immediate (0–60 min):** Activate State HQ as a single point of truth; issue holding statement in multiple languages; publish route and safety advisories; schedule hourly updates.
- **Sustained (2–24 h):** Release time-stamped factual updates; issue myth–fact cards; enable controlled pool access where safe; coordinate with District Administration for curfew or traffic messages.
- **Include:** Public-order instructions, helplines, safety zones.
- **Exclude:** Unverified motives, group labels, emotional adjectives, and selective visuals.
- ***Sample Line:*** *"Multiple calls were received regarding tensions in [area]. Forces are deployed. Please follow official advisories issued hourly at [handles]. Avoid speculation."*

B. Terror Incident / Explosive Threat

- **Trigger:** Confirmed IED threat, ongoing counter-terror operation, or central-agency lead.
- **Immediate:** Delay operational details; mark safety perimeters; release emergency helplines; coordinate with central agencies.
- **Sustained:** Publish only central-agency-cleared updates; withhold suspect names until authorised; issue debrief only after tactical closure.
- **Include:** Perimeter and evacuation guidance.
- **Exclude:** Tactics, device details, suspect descriptors, or security-method references.
- ***Sample Line:*** *"An operation is underway in [zone]. Please avoid the area and follow verified guidance from authorities. Updates will be shared once cleared by the lead agency."*

C. Custodial Death

- **Immediate:** Confirm occurrence; initiate statutory actions (magisterial inquiry, NHRC/SHRC intimation); assign family liaison officer; appoint neutral SPOX.
- **Sustained:** Provide only procedural updates; avoid speculation on cause; ensure dignity of the deceased and sensitivity to family.
- **Include:** Inquiry steps, liaison contact, procedural timelines.
- **Exclude:** Witness identities, medical opinions, or evidentiary details. ***Sample Line:*** *"A death in custody occurred at [PS] on [date/time]. A magisterial inquiry is underway and statutory intimations have been sent. Procedural updates will be shared."*

D. Cyber Breach / Leak of Police Data

- **Immediate:** Confirm scope and nature; isolate compromised systems; liaise with CERT-In/State CERT; issue citizen advisory on precautions.
- **Sustained:** Provide updates on service restoration; commit to post-incident transparency without disclosing technical details.

- **Include:** Service availability, citizen reporting options.
- **Exclude:** IP logs, access tokens, passwords, or architecture details. ***Sample Line:*** *"A cyber incident affected [service]. We are working with competent agencies. Please use [alternate channel] and refrain from sharing OTPs or passwords."*

E. Sexual Offence Against a Minor

- **Immediate:** Ensure survivor anonymity; comply with POCSO confidentiality; provide verified helplines and counselling contacts; coordinate with Child Welfare authorities.
- **Sustained:** Limit statements to procedural progress; never share identifiable or relational details.
- **Include:** Survivor support and procedural assurances.
- **Exclude:** Identities, locality, or timelines enabling re-identification. ***Sample Line:*** *"An FIR under POCSO has been registered. Survivor's identity and location will not be disclosed. Support is being provided. Updates will remain procedural."*

F. High-Profile Arrest

- **Immediate:** Confirm arrest, sections invoked, and due-process steps; prohibit photos or "perp walks."
- **Sustained:** Communicate only procedural milestones (remand, court production). Avoid adjectives or inferences of guilt.
- **Include:** Date/time, legal sections, next step.
- **Exclude:** Confession claims, witness names, and alleged motives. ***Sample Line:*** *"An arrest was made on [date/time] under [sections]. The person will be produced before the court as per the law. No further details can be shared."*

G. Disaster / Mass Casualty Event

- **Immediate:** Conduct joint briefing with Disaster Management; publish helplines, shelters, medical-assistance points, and route advisories.

- **Sustained:** Schedule frequent updates; share casualty numbers only after verification ("as per [authority] at [time]"); maintain a missing-persons desk; consider pool coverage for transparency.
- **Include:** Shelters, helplines, diversion routes.
- **Exclude:** Victim visuals, names, or speculative figures. ***Sample Line:*** *"A coordinated response is underway with Disaster Management. Helplines: [numbers]. Avoid [routes]. Updates every [interval]."*

H. Public Assembly / Protest

- **Immediate:** Publish route advisories, lawful restrictions, and safety precautions; use neutral, de-escalatory tone.
- **Sustained:** Continue time-stamped updates; issue factual post-event summary (detentions, diversions) without attributing motive or judgment.
- **Include:** Traffic, safety, and restriction details.
- **Exclude:** Characterisations, political labels, selective visuals. ***Sample Line:*** *"Public assembly at [location] from [time]. Please use alternate routes [list]. Restrictions under [law] apply. Cooperation is appreciated for public safety."*

I. Suicide / Self-Harm Incident

- **Immediate:** Exclude details of method, location, or personal background; share mental-health helplines; avoid imagery.
- **Sustained:** Remove or anonymise posts that risk imitation; circulate general well-being information.
- **Include:** Helplines, verified support networks.
- **Exclude:** Personal identifiers or speculative causes. ***Sample Line:*** *"We request privacy and sensitivity. If you or someone you know needs support, contact [helplines]. Further details will not be shared."*

J. Missing Person / Child

- **Immediate:** Secure guardian consent (for minors); craft BOLO notice with minimal identifiers and broad locality.
- **Sustained:** Update timeline on recovery or closure; document takedown once person is found.
- **Include:** Contact channels and helplines.
- **Exclude:** Home/school addresses, routine details, or sensitive photos. ***Sample Line:*** *"Help locate [a child/adult] last seen near [area] at [time window]. If seen, contact [number/email]. Please avoid circulating unverified images."*

K. Data Rumour / Misinformation Surge

- **Immediate:** Release myth–fact card with verified information and citations; mark official handles for continued updates.
- **Sustained:** Maintain single-thread authoritative posts; coordinate with PIB or State Information Department; refrain from replying to individuals.
- **Include:** Reference to official press note or order.
- **Exclude:** Speculative rebuttals or ad-hoc debates. ***Sample Line:*** *"Incorrect information is circulating about [topic]. Fact: [verified statement]. Refer to Press Note [ID]. Updates here: [handle]."*

L. Court-Directed Restrictions

- **Immediate:** Circulate the order internally; issue holding line strictly within court's wording; record compliance.
- **Sustained:** Route all media queries to the Legal Vetting Officer; post only content cleared by court; maintain archive of orders and corresponding statements.
- **Include:** Reference to court supervision.
- **Exclude:** Interpretations, paraphrasing, or commentary. ***Sample Line:*** *"A court order governs public reporting in this matter. We are complying fully and will share permissible updates via official channels."*

17.3 Roles and Approvals

- **Spokesperson (SPOX):** Leads drafting, approval, and delivery of messages.
- **Legal Vetting Officer:** Ensures compliance with privacy, contempt, and sub judice laws.
- **Digital Communications Officer (DCO):** Publishes updates, manages accessibility, and archives content.
- **Archivist:** Logs version, timestamp, and corrections for audit.
- **CP/DGP or Lead Agency:** Final authority for high-risk scenarios or inter-agency coordination.

  Each action must be logged in the crisis tracker with the time of approval, publication, and correction (if any).

17.4 Metrics and Exit Criteria

Performance evaluation includes:

- Average time to first holding statement.
- Misinformation-correction latency;
- Accessibility compliance (captions, bilinguality);
- Volume and reach of verified updates;
- Reduction in rumours or hostile virality indicators; and
- Media feedback on accuracy and clarity.

A crisis communication phase formally concludes when:

(a) verified updates stabilise public discourse.

(b) misinformation rate drops below baseline thresholds; and

(c) control reverts to routine Media Briefing Cell operations.

The MBC must then initiate an After-Action Review and integrate lessons into updated playbooks and training modules.

CHAPTER 18. TRAINING AND ACCREDITATION

Systematic training builds a professional culture of lawful, ethical, and empathetic communication. Accreditation provides the mechanism to ensure that only trained and verified personnel interact with the media on behalf of the police.

18.1 Annual Certification Regime

- Every officer designated as a Spokesperson (SPOX), Investigating Officer (IO) likely to engage with media, Digital Communications Officer (DCO), or on-scene Public Information Officer (PIO) shall complete annual certification in communication standards.
- The curriculum comprises a minimum of twelve instructor-led or e-learning hours, followed by written and practical assessments. Certification is valid for twelve months and must be renewed annually.
- A mid-year refresher becomes mandatory after any major incident, change in legislation, or policy update issued by State HQ.
- The objective is to create a trained cadre capable of communicating accurately, neutrally, and within the bounds of law.

18.2 Curriculum Overview

The course blends doctrinal understanding with field realism. Modules include:

- **Legal and regulatory frameworks** — privacy, fair-trial and sub judice limits, contempt of court, and restrictions under the IT Act, RTI Act, and data-protection laws.
- **Ethics and neutrality** — professional restraint, avoidance of political alignment, and sensitivity to community impact.
- **Trauma-informed communication** — survivor-centric approaches and coordination with counsellors or child-welfare officers.

- **Accessibility and inclusion** — use of captions, alt-text, plain language, bilingual content, and standardised icons.
- **Data protection and platform governance** — responsible handling of personal information, password hygiene, and content takedowns.
- **Misinformation response** — verification tools, myth–fact cards, and engagement strategy during digital crises.
- **Practical simulations** — mock press conferences, drafting drills, and social-media scenario exercises.

18.3 Assessment and Rubrics

Assessment consists of two parts:

1. **Knowledge test** through multiple-choice and short-answer questions assessing comprehension of legal limits, institutional procedures, and ethical reasoning.
2. **Practical evaluation** through real-time drafting and oral simulations, including preparation of a press note, on-camera briefing, and social-media update. Evaluation rubrics measure neutrality of tone, precision and factual accuracy, quality of redaction, adherence to timelines, accessibility compliance, and teamwork under pressure. Officers scoring below the threshold must complete remedial modules before certification.

18.4 Training-of-Trainers (ToT) and Cadre Building

- Each range or district nominates a certified trainer responsible for cascading instruction to subordinate units. Trainers receive standard slide decks, cue cards, case studies, and an evaluation script to ensure consistency.
- A state-level trainers' forum hosted by the Police Academy enables exchange of lessons, updates on case law, and discussion of evolving media-technology challenges.
- Quarterly webinars and newsletters support continuing professional development.

18.5 Records and Compliance

- The MBC maintains a **Training Register** containing the names of participants, course dates, modules covered, assessment results, and follow-up actions. Certification status directly determines eligibility for SPOX, PIO, or DCO roles.
- Supervisory officers review training compliance during annual inspections. Persistent non-attendance or expired certification results in temporary withdrawal from communication duties until requalification.

18.6 Media Accreditation Policy

- Accreditation ensures that only bona-fide journalists with verified credentials access police briefings and scenes.
- Applicants must provide identity proof, organisation details, contact numbers, and a signed acknowledgement of the media code of conduct.
- The process follows a transparent sequence: **application → verification → card issuance → one-year validity → renewal with updated documents.**
- Suspension or revocation may occur for misuse of credentials, safety violations, or interference within restricted areas.
- Reasons for any suspension are recorded and communicated in writing. An appeal may be filed within thirty days to the DGP or an authorised review committee.

18.7 Pool Access Agreements

- Where space or safety limits media presence, pool access agreements specify the number of representatives and sharing obligations.
- A single crew captures footage or photographs for collective use by all accredited media present.
- Terms of use, time limits, and attribution rules are documented before access. Breaches of the agreement may result in suspension for up to six months.

18.8 Safety Briefing for Accredited Media

All accredited journalists receive incident-specific safety advisories prepared by the MBC. Key instructions include:

- No entry beyond the marked inner cordon or evidence perimeter.
- Compliance with drone and aerial-footage restrictions.
- Prohibition on filming victims, juveniles, or undercover personnel.
- Mandatory use of visible press identification at all times.
- Adherence to evacuation and emergency alert protocols announced on site. These briefings are reissued during major operations or disasters and archived for reference.

CHAPTER 19. MONITORING, CORRECTIONS, AND REJOINDERS

Active and systematic monitoring protects factual accuracy, ensures prompt correction of misinformation, and sustains public confidence in police communications. The framework combines real-time responsiveness with respect for freedom of the press and lawful expression.

19.1 Monitoring Architecture

- Every Media Briefing Cell (MBC) shall establish a **Monitoring Desk** equipped with tools and trained staff to capture, analyse, and respond to information circulating in traditional and digital media.
- Inputs include newspaper articles, online news items, television bulletins, social-media posts, messaging-app forwards, and verified citizen submissions.
- The desk operates a **single digital ticketing system** through which every flagged item is registered, assigned to an officer, actioned, and closed with timestamps. This enables traceability from detection to resolution.

Monitoring officers prepare a **daily situation summary** noting:

- containing factual inaccuracies or prejudicial commentary;
- items emerging misinformation trends;
- tone and framing of coverage across outlets;
- community-sentiment indicators relevant to public order; and
- high-reach influencers or handles amplifying false narratives.

These summaries feed into weekly reports for the State HQ MBC and the Public Relations Wing for coordinated response and trend analysis.

19.2 Severity and Triage

Each detected issue is rated for **severity and urgency** using a four-tier scale:

Level	Description	Response Timeline
S1 – Minor	Non-material wording or contextual error without impact on perception or safety.	Within one working day.
S2 – Moderate	Factual error that could mislead but causes no immediate harm.	Within eight hours.
S3 – Serious	Violation of privacy, fair-trial risk, or potential contempt exposure.	Within sixty minutes.
S4 – Critical	Large-scale misinformation or imminent public-safety risk.	Immediate—within thirty minutes.

Severity rating guides escalation. S3 and S4 cases trigger automatic alerts to the SPOX, Legal Vetting Officer, and CP/DGP secretariat. If the item relates to national security or communal tension, it is also shared with State Information Department for unified messaging.

19.3 Scope of Monitoring

The MBC may monitor only publicly available information and shall not intercept private communications. All monitoring activities comply with data-protection principles and lawful purpose limitations. Analysts must avoid viewpoint discrimination and assess only accuracy, legality, and risk—not editorial opinion or criticism.

19.4 Correction, Rejoinder, and Legal Notice

- A **correction** is issued when the police themselves have misstated or omitted information.

  A **rejoinder** clarifies factual inaccuracies published by external entities. Both instruments must remain neutral, verified, and non-adversarial.
- Corrections are prioritised; prompt acknowledgment of error enhances credibility. Rejoinders are crafted only after confirming that the misstatement affects public understanding, safety, or rights.
- **Legal notices** are the remedy of last resort—used only where sustained publication causes demonstrable prejudice, breaches confidentiality, or violates a court order. Even then, language must remain proportionate and courteous, upholding the principle of media freedom under Article 19(1)(a).

19.5 Rejoinder Workflow

The rejoinder process follows a mandatory sequence:

1. **Intake and Registration** – The flagged item is logged in the ticketing system with source link, date/time, and summary.
2. **Verification** – Cross-check against official press notes, FIR details, or court orders to determine variance.
3. **Drafting** – Prepare concise clarification quoting authoritative facts and Press Note IDs. Tone must remain procedural, not defensive.
4. **Legal Vetting** – Review for accuracy, privilege, and risk of contempt or defamation.
5. **Approval** – SPOX or CP/DGP approves text and mode of dissemination.

6. **Dispatch** – Send to the concerned media outlet with a polite request for update; optionally publish on official handles tagged to the original post for transparency.
7. **Archival** – Store the final rejoinder, correspondence, screenshots, and timestamps in the MBC archive for audit.

Where multiple outlets repeat the same inaccuracy, one consolidated rejoinder referencing the official release should suffice.

19.6 Template — Neutral Rejoinder

"This is to clarify verified facts concerning [incident]. The authoritative details are contained in Press Note [ID] dated [DD/MM/YYYY]. We request that the record be updated to reflect the verified information. Our purpose is to ensure accuracy and prevent misunderstanding."

19.7 Escalation and Coordination

In high-risk or fast-moving situations, the Monitoring Desk escalates directly to the State HQ MBC for coordinated messaging with other departments (Information, Home, Disaster Management). All rejoinders involving communal, terror, or custodial matters require Legal Vetting Officer clearance before issue. If the misinformation originated from official or political sources, HQ refers the matter to the competent authority for appropriate clarification.

19.8 Monthly Dashboard and Analytics

Each month, the MBC compiles an analytics dashboard capturing:

- total corrections and rejoinders issued;
- average response time;
- misinformation clusters neutralised;
- accessibility compliance rate (captioned videos, bilingual posts);
- takedowns executed with legal basis;
- training gaps identified;

- number of legal notices served, categorised by ground (privacy, contempt, operational secrecy).

Trends are reviewed in the Monthly Compliance Meeting. A public summary—anonymised by outlet—is published quarterly on the official website to reinforce transparency.

19.9 Lessons-Learnt and After-Action Reviews

After major incidents, the SPOX convenes an **After-Action Review (AAR)** within seventy-two hours. The AAR assesses:

- timeliness and clarity of first statement;
- adequacy of fact-checking and redaction;
- tone of engagement with media and public;
- correction latency;
- secondary misinformation created by silence or ambiguity; and
- overall impact on public trust.

Findings are summarised in an AAR Note, approved by the CP/DGP, and shared with training and policy units. Patterns of recurring error trigger updates to templates, refresher sessions, or amendments to SOPs.

19.10 Ethical and Privacy Considerations

Monitoring and correction must never be used to suppress legitimate criticism or commentary. All actions must be confined to verifiable inaccuracies or clear legal breaches. Analysts and SPOX officers are personally responsible for upholding neutrality, avoiding selective response, and preserving a written audit trail for every intervention.

CHAPTER 20. DISCIPLINE AND ACCOUNTABILITY

Discipline underpins public trust in police communication. It transforms the Manual's principles into enforceable standards of conduct and ensures breaches are dealt with fairly and proportionately.

20.1 Principles

The disciplinary system rests on three values, **fairness, proportionality, and transparency.**

Mistakes made in good faith are treated through coaching and remedial training. Deliberate misconduct—such as leaks, prejudicial statements, or unauthorised political commentary, attracts proceedings under the State Police Conduct Rules. Penalties increase for repetition or wilful disregard of directions. Discipline aims at reform, not punishment alone.

20.2 Categories of Violations

1. **Negligence:** minor formatting, spelling, or timing errors causing no harm.
2. **Procedural Non-Compliance:** failure to seek legal vetting, incomplete archives, or missed approvals.
3. **Substantive Breach:** prejudicial comment, privacy violation, or disregard of sub judice restriction.
4. **Gross Misconduct:** deliberate leak of confidential data, political messaging, or defiance of court or departmental orders.

20.3 Progressive Discipline Matrix (Illustrative)

Instance	Action	Follow-up
First instance (negligence)	Coaching, verbal or written reminder	Review after 30 days

Instance	Action	Follow-up
Repeat/ substantive breach	Formal warning; removal from SPOX/PIO duties; mandatory retraining	Audit by superior officer
Gross misconduct	Suspension pending inquiry; charge-sheet under Conduct Rules; penalties as prescribed	Findings archived with reasons

Each proceeding records factual details, intent, impact, and remedial steps to uphold procedural integrity.

20.4 Fair Process and Documentation

- The officer is notified in writing of the alleged violation, provided copies of evidence, and allowed a reasonable opportunity to respond.
- A designated Inquiry Officer conducts fact-finding, maintaining a chain of custody for digital artefacts such as emails, recordings, or social-media screenshots.
- Proceedings remain confidential, proportionate, and time-bound. Final orders and evidence inventories are filed in the personnel dossier and reviewed annually for learning value.

20.5 Remediation and Prevention

Where non-compliance reveals systemic gaps, remedial actions include:

- targeted refresher training or mentorship;
- revision of templates and SOPs;
- periodic audits of sensitive communications; and
- rotation of officers repeatedly exposed to high-pressure media duties.

Departments submit compliance certificates to State HQ confirming closure of disciplinary loops and prevention measures adopted.

20.6 Transparency to the Public

- Quarterly anonymised summaries are published outlining the number, type, and status of infractions, actions taken, and training completed. Names are disclosed only when required by the court or oversight authority.
- Such disclosure demonstrates institutional accountability while protecting individual fairness and morale.

20.7 Linkage to Performance and Recognition

- Units maintaining year-long zero-breach records and timely correction performance may be recognised in annual communication-excellence citations issued by State HQ.
- Positive reinforcement encourages ethical practice and continuous improvement.