NPCC
National Police Chiefs' Council

Information Disorder:

Strategic Risk Guidance v.1.1

NPCC Strategic Hub

February 2026

Contents

1. Summary

1.1. This document provides guidance, suggestions and examples to support forces in identifying, articulating and recording strategic risk assessments in relation to Information Disorder via the presentation of mis, dis & malinformation (MDM).

1.2. The NPCC Strategic Risk Assessment (national articulation, January 2026) reads:

1.2.1. Instances of widespread MDM continue, particularly online and in relation to socio-political issues; where false narratives are created, adopted and spread rapidly. Mis, dis and malinformation has increasingly impacted on UK policing operations, delivery, priorities and public perception; with recent examples of MDM contributing to social tensions and public disorder, increased threat, risk & harm and vulnerability/safeguarding concerns.

1.2.2. There is a risk that continued instances of MDM (particularly unmanaged occurrences) will continue to impact policing operations/delivery, and failure to address these challenges could erode public trust, hinder effectiveness during crises, and leave policing vulnerable to the impact of public misunderstanding, and purposeful manipulation by malicious actors. This could ultimately compromise public safety, damage community relations, and undermine the legitimacy of law enforcement in the UK and globally.

1.3. The NPCC Strategic Planning and Performance team (SPP), the National Risk Management Forum (NRMF) and the NPCC Information Disorder portfolio recommend that all forces consider the requirement for a strategic risk entry on local strategic risk registers/logs.

1.4. This document offers support to risk leads, practitioners and chief officers, to review and consider the force position in line with local risk signals and existing controls.

1.5. The document makes suggestions on risk articulation and recording, and potential positions/baselines for common components used in a variety of risk frameworks/approaches.

1.6. The components have been selected with reference to NPCC adopted practice, ISO31000[1] guidance, the Home Office Orange Book[2] and engagement with forces, to best support the potential variety of force strategic risk frameworks and formats currently in place.

[1] ISO 31000:2018 - Risk management — Guidelines
[2] Orange Book - GOV.UK

1.7. Suggested components and positions should be considered as a 'baseline' to sense check local force risk landscapes, rather than as a directive on how forces should record their own risk entries.

1.8. For support on using this guidance, or for general queries on strategic risk assessment or processes, please contact **S31(1)**

2. Strategic Risk Components (Guidance)

2.1. Strategic Risk Title

- Impact of Information Disorder on Policing Operations, Trust & Public Safety.

2.2. Risk Owner(s)

- Chief Officer or Chief Officer Group (COG).
- Appropriate business area lead - Head of Risk, Corporate. Communications, Force Intelligence Lead, Legal etc.
- Consider joint accountability across chief officers and/or senior leadership within key business areas, as necessary.

2.3. Risk Description

2.3.1. Version 1: Cause, Event, Effect

- Cause: Rapid online spread of false/misleading or weaponised information about force activity, priority incidents, investigations, protests or contentious cases, amplified by platform algorithms and coordinated actors.
- Event: Material MDM incident (flashpoint or cascade) overwhelms official comms capacity; vacuum exploited by hostile or opportunistic actors; mislabelling of suspects/events; coordinated harassment/doxxing; calls to violent action.
- Effect: Public disorder and community tension; harm to victims/witnesses; threats to officer/public safety; operational disruption and evidential prejudice; surge demand on contact centres; loss of legitimacy and trust; financial impacts (mutual aid, overtime, claims); ongoing distribution of misinformation which negatively affects policing's response.

2.3.2. Version 2: Situation, Relevance, Impact (NPCC standard)

The rapid spread of mis, dis and malinformation - especially during fastmoving major incidents (flashpoints) or high relevance periods (political processes, national events) - continues to increase and escalate. When widespread, MDM routinely outpaces lawful, fact-based communication, exploiting disclosure constraints, influencing social narratives, increasing social tensions and eroding public trust.

Information Disorder presents an increased risk of public disorder, threats to officer and community safety, operational disruption, financial burden, reputational harm, and reduced ability to maintain confidence and deliver effective policing during critical incidents.

2.4. Inherent (Uncontrolled/Reported) Risk Assessment

2.4.1. The suggested position of inherent risk is based on an assumed variation of a 5x5 matrix.

		Impact				
		Very Low	Low	Moderate	High	Very High
Likelihood	Very Low	1	3	5	8	10
	Low	2	6	12	14	17
	Moderate	4	11	15	19	21
	High	7	13	18	22	24
	Very High	9	16	20	23	25

Table 1. NPCC Risk Scoring Matrix, RMF v3 (Reference Only).

2.4.2. The baseline reflects national assessment of impact to forces and should be tuned using local risk signals and horizon scanning e.g. community tensions, protest activity, elections schedules, force capability, stakeholder engagement or existing control maturity.

- **Likelihood Level: High.** Forces should expect at least one significant Information Disorder event intersecting with a force's caseload (major crime, protest, critical incident) given recent UK patterns and platform dynamics[3].

- **Impact Level: High.** Potential for widespread disorder, operational impact, reduced public safety, multi-agency mobilisation, reputational harm or compromised justice outcomes.

2.4.3. The NPCC risk management framework utilises a 5x5 scoring matrix, with unique value scoring. The NPCC strategic risk assessment reflects a high ('level 4') position for both likelihood and impact, resulting in a score of 22 and 'very high' categorisation.

[3] Social media, misinformation and harmful algorithms (UK Parliament)

2.5. Causes and Impacts

2.5.1. Causes

- Rapid viral spread of false narratives on social media, especially immediately after major incidents (e.g., Southport 2024 false identity claims).
- Algorithmic amplification of harmful and sensational content, increasing visibility of false narratives beyond official factual updates and the reinforcement belief of false narratives which can lead to extreme acts.
- High-reach influencers and extremist networks actively promoting disinformation to mobilise supporters or provoke unrest.
- Politicisation of policing and polarising social issues.
- AI-generated and synthetic content (images, videos, posts) accelerating spread and believability of false claims, reduced confidence, diminished 'truth'.
- Coordinated mobilisation and opportunistic exploitation of narratives, often using online channels to organise offline action.
- Hostile foreign information operations attempting to manipulate public sentiment and exploit domestic tensions.
- Platform policy gaps and slow moderation response, where harmful content remains live long enough to influence public behaviour.
- Low media literacy and high susceptibility among parts of the public, increasing vulnerability to misinformation during high-tension events.

2.5.2. Impacts

- Rapid escalation to public disorder, including riots, incidents perceived to be motivated by hate, and targeted attacks on community locations (e.g. religious sites, government buildings, asylum accommodation).
- Increased threats to officer safety, including hostility, harassment, and doxxing, driven by false claims about policing behaviour.
- Operational disruption and resourcing strain, requiring surge deployments, mutual aid, and diversion of officers from core duties.
- Loss of public confidence and trust, as misinformation about policing actions or intent undermines perceived legitimacy.
- Loss of internal trust and confidence, as these narratives can impact on staff wellbeing, safety and attrition.
- Damage to community cohesion, with false narratives inflaming tensions between demographic, religious, or political groups. These issues can also manifest differently, to greater or lesser extents, depending on the geographic locations of communities.
- Increased pressure on contact centres and engagement teams, as misinformation drives spikes in public concern and misinformation reporting.

- Potential prejudice to investigations and court proceedings, due to uncontrolled release of false or misleading suspect information.
- Reputational harm, including scrutiny of force communications, perceived inconsistency, or delayed responses during crises.
- Amplification of extremist narratives, increasing radicalisation risks and fuelling longer-term hostility toward communities or institutions.

2.6. Impact Proximity

2.6.1. **Already Encountered** – the anticipated impact of the situation has already been encountered in part or in full[4].

2.6.2. Based on national engagement, forces are likely to have already encountered at least one instance of negative impact directly, or indirectly, influenced by MDM. Local tuning should assess any previous instances and align impact proximity with the force assessment of likelihood (2.4.2) if not already encountered.

2.6.3. Risks associated with MDM are contained within the Government's Chronic Risk Analysis[5]. Chronic risks are defined as 'longer-term challenges that erode our economy, community, way of life and/ or national security' and MDM's inclusion as a chronic risk, recognises the long term issues and future risk of information disorder, with the potential for significant impact, severe enough to require critical response from the UK policing, public sector and civil contingencies systems.

2.7. Treatment

2.7.1. **Treat/Transfer** – forces are advised to adopt a combined treat (reduce) and transfer (share) approach to this risk, looking to minimise the unmanaged risk and to seek engagement and support with partners, stakeholders, responsible bodies and national functions.

2.7.2. **Treat (Reduce):**

- Improve clarity, speed and reach of force communications.
- Strengthen digital monitoring and surge capability.
- Clarify decision making routes around disclosure, legal constraints, suspect detail guidance, and community engagement.
- Ensure operational readiness to respond to disorder triggered by harmful online narratives.

[4] NPCC Risk Management Framework v3.
[5] Chronic risks analysis - GOV.UK

2.7.3. **Transfer (Share):**

- Formalise escalation routes to platforms, Ofcom, and relevant government teams.
- Deepen collaboration with other emergency services, local authorities, civil-society partners and trusted community messengers.
- Engage national policing structures to ensure consistency and access to specialist support.

2.8. Risk Appetite

2.8.1. Where a force is utilising risk appetite within its framework, the NPCC has suggested a differentiated risk appetite, recognising that some exposure to MDM is unavoidable, but that unmanaged exposure can significantly threaten public safety, operational effectiveness and legitimacy. Appropriate risk appetite levels may therefore benefit from reflecting both the need for transparency and the requirement to safeguard investigations, the public, legal rights and community cohesion.

Appetite	Summary
Averse	Significant avoidance of risk. Removal of risk as a priority. Extremely low tolerance for uncertainty. Lowest risk options always preferred choice. Extreme reluctance to compromise on risk. Consider 'Very Low' to 'Low' target risk
Cautious	Avoidance of risk. Reduction of risk as a priority. Low tolerance for uncertainty. Will accept essential risk if limited likelihood/ impact of failure. Reluctance to compromise on risk.
Moderate	Preference for safe delivery, consideration of some risk. Will take strongly justified risks Limited tolerance for uncertainty. Will accept risk if likelihood heavily outweighed by benefits. Willing to compromise only if it's the current best option for delivery.
Open	Will take justified risks. Willing to operate with some uncertainty. Will accept risk if likelihood heavily outweighed by benefits. Willing to compromise, at risk of failure, to increase chance of delivery. Consider 'Moderate' to 'High' target risk.
Brave	Will take risks. Fully anticipate and accept uncertainty. Will choose the option with the greatest positive outcome; accept possibility of failure. Willing to compromise other goals/ risk failure. Consider 'High' target risk.

Table 2. NPCC Risk Appetite, RMF v3 (Reference Only).

2.8.2. **Communication Transparency – Cautious to Moderate (or equivalent)**

- Forces should maintain a Cautious to Open appetite for timely, fact-based communication.
- Forces may be required to take controlled and reasoned risks in providing early, verified information to reduce information vacuums and minimise the spread of harmful narratives.

- This may include proactively explaining legal constraints and clearly differentiating between confirmed facts, context and what cannot yet be disclosed.

2.8.3. **Public Safety, Community Cohesion and Justice Outcomes – Averse (or equivalent)**

- Lowest appetite for risk in relation to core duties around public safety, officer safety, community cohesion, and the integrity of investigations.
- The force is likely to be unwilling to accept exposure to Information Disorder that could foreseeably lead to
  - escalation to disorder;
  - targeted hostility or hate crime;
  - operational disruption or harm;
  - damage to community confidence;
  - reduced public trust & confidence;
  - reduced legitimacy or effective of policing;
  - or prejudice to judicial proceedings.
- Where reduced transparency is necessary to protect these areas, forces must communicate this explicitly and proportionately.

2.9. Key Risk Signals & Indicators

2.9.1. **Emerging & Opportunistic Narratives**:

- Increasing trends, or sudden spikes after an incident (flashpoints), in online speculation on policing matters - particularly around perpetrator demographics, suspect identity, motives or police response (consistent with patterns leading to the 2024 Southport riots).
- New or unverified 'first claims' or inside knowledge spreading quickly, such as viral false identity narratives that fuelled unrest.
- Narratives exploiting known information vacuums, especially when police cannot lawfully disclose details due to legal and investigative duties.

2.9.2. **Social Media & Amplification**:

- High-velocity sharing on major platforms, where recommendation algorithms push inflammatory, high impact, high engagement MDM content at scale.
- AI-generated or synthetic content, increasing believability and reach of false claims.
- Trending hashtags linking an incident to political or ideological narratives (e.g. anti-migrant or anti-police framing observed in 2024).

2.9.3. **Actor Related Signals**:

- Extremist/divisive accounts seeding or amplifying content, including those previously observed mobilising disorder.
- High-reach influencers or verified accounts promoting unverified claims.

- Coordinated behaviour across channels and platforms.

2.9.4. **Offline Activity & Mobilisation**:
- Online calls for gatherings, protests, or “defence actions” near key sites or civic buildings.
- Spike in hate-related discourse or targeted hostility, often a precursor to real-world tension escalation.
- Circulation of broad, sweeping claims about policing behaviour, legitimacy, structures or processes e.g. “two-tier policing” narratives.

2.9.5. **Operational Stress Signals**:
- Increased public contact centre traffic, driven by confusion or fear based on false narratives (noted across forces during major misinformation cycles).
- Early signs of reputational harm, including rapid spread of distrust-laden narratives or accusations of inaction/misconduct.

S40(2) **(Strategic Planning and Risk Manager)**

NPCC Strategic Hub, on behalf of

ACC Arman Mathieson, NPCC Information Disorder Portfolio Lead