Managing information disorder

This page is from APP, the official source of professional practice for policing.

First published 23 February 2026

This APP provides general principles for police management of information disorder, insofar as it may have an impact on public safety and policing operations. This guidance focuses on the critical incident and communications response. It does not replace operational or investigative practice, nor does it provide detail on covert monitoring, which requires specific authorities.

Risks of information disorder

Inaccurate information online can:

- threaten the safety of individuals, communities, businesses and policing operations
- increase hostility towards police officers and risk their safety
- erode trust and impede engagement with communities, as well as criminal justice outcomes

Misinformation, disinformation and malinformation are three types of information disorder that can cause such harm.

- Misinformation is false or inaccurate information shared without the intent to cause harm.
- Disinformation is false or inaccurate information shared deliberately to mislead or cause harm.
- Malinformation is information rooted in truth but exaggerated, taken out of context or used to cause harm.

Information disorder strategy

To manage the risk of information disorder, policing leaders should establish systems to monitor, access and counter information disorder. This should include, but is not restricted to, the following stages.

Prepare

- Recognise and make provision for proactive communications across a range of reliable channels and platforms to help prevent misinformation, disinformation and malinformation.

- Establish monitoring, assessment and triage capability, with timely escalation routes into command structures.
- Operate a risk assessment framework to manage responsibility for **issuing public communications**.
- Train roles relevant to both overt and covert social media, monitoring how to identify and escalate potential information disorder requiring police action.

Identify

- Monitor relevant channels and triage relevant information.
- Log incident and relevant information – for example, source, time, channels, content and initial reach.
- Escalate based on force protocols for operational risk assessment, in liaison with the corporate communications department (CCD) where required.

Assess

- Assess the likelihood, scale and potential impact to public safety, investigations and public trust.
- Consider all elements of risk including, but not restricted to:
  - source and intent
  - motivation
  - scale
  - velocity
  - channel
  - audiences
  - timing
  - content characteristics – for example, emotive language, call to action
  - legal and operational constraints
- Factors to consider can be found in **Critical incident management APP**.
- Include these risks within the community impact assessment (CIA), where a CIA is undertaken.

Decide

If a policing response is deemed necessary, it is likely to fall into one or more of the following four categories for response.

- Critical incident: Immediate response and senior oversight.
- Manage risk: Corrective public messaging and targeted engagement.
- Prevent at source: Platform reports, takedown or counter-narratives coordination with partners.
- Watch closely: No active response but continued monitoring if required.

Respond

Tactics should be used proportionately and should avoid amplifying falsehoods. They include, but are not limited to:

- rapid factual statements via paid, earned, shared and owned (PESO) channels
- corrections and clarification on force channels and via partner outlets and trusted voices
- platform reporting and requesting that content containing falsehoods is taken down, where it breaches terms or endangers safety and it is the role of police to do so
- targeted community engagement and liaison with local leaders and media
- legal action or disclosure to investigating team where relevant

Refer to the Government Communication Service's **RESIST 2 counter disinformation toolkit** for detailed tactical options.

Evaluate

Assess the effectiveness of the action, fully review and refine tactics as required.

General principles

- Not all misinformation, disinformation and malinformation requires a policing response; the decisions need to be made locally. This on a case-by-case basis.
- Senior operational leads should consider whether policing is the right agency to respond and if doing so would have an impact on legitimacy and the requirement for independence and impartiality.
- Prioritise where safety, investigations or public trust are at risk. Where false or manipulated information has been identified and assessed to have an impact on public safety or public trust in policing, steps should be taken to act swiftly to avoid false information spreading unchallenged.

- Ensure that monitoring is sufficient or that it can be escalated out of hours for critical incidents.
- During critical or major incidents, the senior operational lead should consider instances where co-locating relevant roles – for example, communications and intelligence leads – will improve the efficiency of monitoring, assessment and response.
- Use wider PESO options to amplify accurate information and enlist trusted intermediaries (media, community leaders and subject-matter experts).
- Consider targeted community engagement when specific individuals, groups or communities are affected.
- Escalate cross-force or national impact incidents to the NPCC and/or the College of Policing.

Tags

APP