

POLICY ON INFORMATION INTEGRITY IN PEACEKEEPING SETTINGS

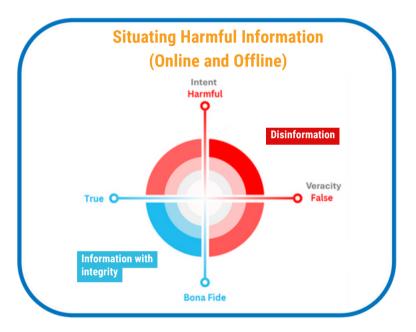
Two-pager Series || #1



2025

WHAT is the policy for?

The policy sets out the approach, principles, roles and responsibilities, and processes by which UN peacekeeping operations and Headquarters will strengthen information integrity and address harmful information, such as misinformation, disinformation and hate speech. It will help peacekeeping to anticipate, mitigate and respond to the risk posed by harmful information.



WHERE does is apply?

The policy applies to peacekeeping operations and the Department of Peace Operations (DPO). It pertains to harmful information in the **online and offline** info environment as they affect:



Safety and security of peacekeepers **Mandate implementation** of each peacekeeping mission.

WHO is it aimed at?

This policy is aimed at peacekeeping practitioners at all levels in the field and HQ. It is of particular relevance to those involved in the monitoring, analysis, response and evaluation cycle. This includes: Strategic Communications, JOCs, JMACs, Political Affairs, Civil Affairs, Human Rights, Protection of Civilians, Gender, Safety and Security, Police and Military components.

WHY is it needed?

False, misleading and/or manipulated information can weaken consent and support for peacekeeping, reduce the political and operational space for mandate implementation, threaten the safety and security of peacekeepers and fuel divisions and stoke violence in host countries. Mis/disinformation and hate speech can also hinder mandate implementation, including support to peace processes and the protection of civilians.

Terms and Definitions

Information Integrity An information ecosystem in which freedom of expression is fully enjoyed and information that is accurate, reliable, free from discrimination and hate is available to all in an open, inclusive, safe and security information environment.

Misinformation Inaccurate information that is unintentionally shared in good faith by those unaware that they are passing on falsehoods.

Disinformation Information that is inaccurate, intended to deceive and shared in order to do serious harm.

Hate speech Any kind of communication in speech, writing or behaviour that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor.

Relevant Legislative Guidance

General Assembly
A/RES/76/274 (2022), A/78/19 (2024)
Security Council

Thematic: 2686 (2023), 2730 (2024) **Mission Specific:** 2759 (2024), 2695 (2023), 2717 (2023)



POLICY ON INFORMATION INTEGRITY IN PEACEKEEPING SETTINGS

Two-pager Series || #1



Monitoring, Analysis, Response and Evaluation Cycle

The Policy on Information Integrity outlines a cycle to **monitor, analyse, respond and evaluate** the information environment, which should guide peacekeeping missions' approach.

Analysis (& Report)

Identify and understand the actors involved in proliferating false content, behaviour consistent with info manipulation tactics and the narrative content (ABC framework)

Monitoring (& Report)

Daily monitoring of the information environment enables situational awareness and contributes to trend and pattern analysis

Response (& Report)

Missions are advised to implement a range of responses, based on analysis (see response measures below)

Evaluation (& Report)

Impact evaluation to be conducted in an ongoing manner to track progress and inform decision making

Guiding Principles

Multidisciplinarity Within parameters of the peacekeeping mandate, a combination of skills and expertise will be applied.

Integrated Effort Whole-of-mission and whole-of-UN approach to enable effective and coordinated action.

Proactive, preventive stance Anticipate and mitigate risks, mindful of human rights.

People-centered Adopt a transparent, inclusive and "do no harm" approach.

Gender- & age-responsive Analysis and responses should consider gender and age-specific roles.

Non-clandestine Actions must align with applicable legal frameworks and human rights; clandestine actions are prohibited.

Respects data protection and privacy Data used must adhere to UN confidentiality and security standards.

Preventive and Response Measures

- Strategic communications
- ✓ Political outreach and commitments
- Community engagement
- Protection of journalists, human rights defenders and media workers
- Public reporting
- Accountability for incitement to hostility, discrimination or violence
- Reporting to technology platforms
- ✓ Supporting long-term societal resilience