Draft Recommendation of the Council on Information Integrity

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development (OECD) of 14 December 1960;

HAVING REGARD to the standards developed by the OECD in the areas of building trust and reinforcing democracy, artificial intelligence, children in the digital environment, digital security, health data governance, internet policy making, open government, privacy, protection of personal data, regulatory policy and governance, support to media and the information environment, transparency and integrity in lobbying and influence, and access to and sharing of data;

HAVING REGARD to relevant international obligations, commitments, and other standards aimed at guaranteeing press freedom and human rights, including freedom of opinion and expression;

RECOGNISING that reinforcing information integrity is essential for exercising the right to freedom of opinion and expression, and that policy interventions should not lead to greater information control by governments;

RECOGNISING that the spread of mis- and disinformation and other forms of information manipulation distorts evidence-based debates and analysis and can undermine the public's willingness and ability to engage in democratic debate, thereby deteriorating the quality of the information environment and public discourse, and posing a fundamental risk for democracies and universal human rights;

RECOGNISING that public policies are a tool to support information environments conducive to the availability of reliable, evidence-based, plural, and timely information sources that enable individuals to be exposed to a variety of ideas, make informed choices, and exercise their rights;

RECOGNISING that public policies that reinforce information integrity are only meaningful and effective in democratic systems where governments adopt and uphold human rights laws, including laws that protect freedom of opinion and of expression, privacy, personal data, and fundamental democratic principles, including the rule of law, the separation of powers including an independent judiciary, free and fair elections, and press freedom;

RECOGNISING that developing and implementing effective legal frameworks and measures for the protection of press freedom and of journalists and media workers, as well as creating and maintaining an enabling environment for journalists to perform their work independently and without fear of reprisal or undue surveillance and interference, is essential to reinforce information integrity;

RECOGNISING that access to information and connectivity are key enablers of information integrity;

RECOGNISING that an open, free, and interconnected internet is crucial to promote freedom of expression and other universal human rights;

RECOGNISING that the emergence of online information platforms and new information and communication technologies have reshaped the information environment and that they can increase access to information, promote citizen engagement, and foster innovative models for news reporting;

RECOGNISING that online information platforms design and implement policies and decisions that affect the spread of content with a wide variety of consequences on information integrity;

RECOGNISING the importance of designing appropriate public policy interventions tailored to the risks, including technology-facilitated gender-based violence, image-based abuse and child cyberbullying, posed by online information platforms, taking into account their diverse size and reach;

RECOGNISING that public policy responses related to specific types of content are particularly complex due to the difficulties in defining "disinformation" and the risks that legislation targeting legal but harmful content can be used to limit freedom of opinion and expression, requiring a nuanced approach with appropriate safeguards for freedom of opinion and expression;

RECOGNISING that governments themselves undermine information integrity if they create or amplify disinformation and information manipulation contrary to obligations that provide for the exercise of human rights, including freedom of opinion and expression;

RECOGNISING that strengthening privacy protections, personal data protections, and creating oversight and accountability mechanisms to ensure compliance with relevant policies by online information platforms, can be important steps to increase transparency in the information ecosystem, as well as give users more visibility and control over what personal data is collected and where and how it is used, sold, or shared;

RECOGNISING that building information integrity requires actors across society − namely the private sector, media and journalists, academia, civil society and governments − to act together to develop comprehensive and evidence-based public policies in support of information integrity;

RECOGNISING the importance of fostering innovation and research to inform public policy responses to the challenges posed by the spread of mis- and disinformation and other forms of information manipulation and their risks to human rights and democracy;

RECOGNISING that policies and decisions should respond to the specific risks posed by children's engagement on online information platforms, and should be designed to help children develop in an environment conducive to the full exercise of their universal human rights, including the rights to freedom of opinion and expression and future ability to foster democratic engagement;

RECOGNISING that the design choices of search algorithms and recommender systems, and the increasing use of advanced Artificial intelligence (AI) systems, in particular generative AI, can have negative implications for information integrity and human rights through the potential for faster, less expensive, and easier creation of realistic content as well as a wider and more targeted dissemination of disinformation, and that this will involve a continued focus on the development of effective standards in this space aimed at guaranteeing human rights;

RECOGNISING that monitoring and measurement of policy implementation, comparative insights into what public policies are in place, and identifying what works and why, including through independent research, is crucial to continuously improve information integrity;

RECOGNISING that technological changes continue to present new opportunities and risks for information integrity, and that new technologies, including AI, can be used in the fight against disinformation and to strengthen information integrity;

RECOGNISING that there is a need to work across national borders and foster international co-operation to strengthen public policy design and implementation that seeks to reinforce information integrity;

RECOGNISING that strengthening information integrity requires public policy responses that evolve over time, with Members and non-Members having adhered to this Recommendation (hereafter "Adherents") adopting initiatives and reforms at varying pace and in different orders, prioritising different policy areas in this Recommendation according to their specific circumstances while prioritising the necessity to keep an open civic space and safeguard freedom of opinion and expression;

On the proposal of the Public Governance Committee:

I. **AGREES** that the purpose of this Recommendation is to provide a comprehensive framework to support Adherents in strengthening information integrity and addressing threats posed by information manipulation in countries with democratic governance and freedom of opinion and expression, and acknowledges that Adherents will implement the Recommendation consistent with their institutional and legal frameworks*.*

II. **AGREES** that, for the purpose of this Recommendation, the following definitions are used:

- **Bot** refers to an automated online account where all or substantially all of the actions or posts of that account are not the result of a natural person, and which can perform tasks such as sharing or interacting with content without direct human intervention.
- **Co-ordinated inauthentic behaviour** refers to the artificial amplification of the reach or engagement of content through a co-ordinated or networked effort, for instance through the creation and use of bots and other fake, impersonated, or misrepresented accounts, often across multiple online information platforms and sometimes facilitated by AI, to manipulate public discourse, deceive users, and pursue illicit activity for financial gain.
- **Disinformation** refers to verifiably false, manipulated, or misleading content that is knowingly and intentionally created and / or shared, including through co-ordinated inauthentic behaviour, to deliberately deceive, manipulate or inflict harm on a person, social group, organisation or country.
- **Foreign information manipulation and interference (FIMI)** refers to deliberate and co-ordinated efforts within the information ecosystem by, or on behalf of, a foreign power or its proxy, in order to interfere, disrupt, confuse, or corrupt the decision-making processes and public discourse in an attempt to further the interests of that foreign power.
- **Information** refers to content that is processed, disseminated, and brought to the attention of the public in general or to a large group of individuals and that is used to make sense of the world.
- **Information integrity** is the result of an information environment that promotes access to accurate, reliable, evidence-based, and plural information sources and that enable individuals to be exposed to a variety of ideas, make informed choices, and better exercise their rights.
- **Information manipulation** refers broadly to the deliberate co-ordinated inauthentic dissemination of information that is falsified, distorted, or taken out of context, often in an effort to magnify polarisation and social division, undermine trust, or cause individual, social and economic harm.
- **Media** refers to services that provide television or radio broadcasts, on-demand audiovisual media services, audio podcasts, and press publications usually with editorial oversight; it does not refer to user-generated content that is not otherwise considered to be created for professional purposes, private correspondence, advertisements, or corporate communication; media outlets refer to the channels or platforms used to share such media.
- **Media and information literacy** refers to the ability for citizens to critically, effectively, and responsibly access, understand, use, and engage with information and media platforms, both online and off-line.
- **Misinformation** refers to verifiably false or misleading information that is shared unknowingly and is not intended to deliberately deceive, manipulate or inflict harm on a person, social group, organisation or country, though the effects of which may cause harm.

- **Online information platforms** refer to digital services that also disseminate information they store to the public, often at the user's request, including, for example, search engines, social media platforms, message boards, app stores, online forums, and gaming and virtual worlds.
- **Personal data** refers to any information relating to an identified or identifiable individual;
- **Public interest media** refers to media that create and distribute content that exists to inform the public about matters that concern them; provides fact-based information in a trustworthy manner; commits to the demonstrable pursuit of truth, for example through sourcing practices and the representation of the audiences it hopes to serve; is editorially independent; and is transparent about processes, finances, and policies used to produce it.
- **Strategic Lawsuits Against Public Participation (SLAPP)** refer to lawsuits that are often disguised as defamation actions or alleged constitutional and/or civil rights violations that are initiated against journalists or civil society organisations to drain resource, intimidate, silence, or restrict the targets' freedom of expression and information regarding matters of public interest or social significance.

Strengthen societal resilience

III. RECOMMENDS that Adherents strengthen societal resilience to misinformation, disinformation, FIMI, and other forms of information manipulation, by:

1. Enhancing individuals' understanding of – and skills to operate in – modern information environments, in particular through policies or initiatives that:

   a. Collaborate with schools, libraries, cultural institutions, civil society organisations, journalists, online information platforms or other private actors, as relevant and appropriate, to design and adopt initiatives for children and adults aimed at: building understanding of misinformation, disinformation, and other forms of information manipulation threats; fostering media and information literacy skills, in particular the ability to evaluate sources of information; raising awareness and promoting skills to identify and understand the potential risks of AI-generated content in the information environment; and strengthening civic and scientific literacy;

   b. Develop and publish materials to build understanding of misinformation, disinformation, and other forms of information manipulation threats;

   c. Promote media and information literacy in school curricula, according to children's developmental stage, from early childhood education to higher education and develop training programmes for teachers;

   d. Share, to the extent possible while protecting sources and methods and other national interests, threat assessments of the information environment, including information on malign actors, examples of relevant attacks and manipulations, methods and target audiences, in an effort to providing reliable information on threats to the public, platforms, researchers, and civil society;

   e. Evaluate, where possible, the impact of media and information literacy programmes and develop research to better understand the experiences of persons and groups who may be in vulnerable situations or are at greater risk of information manipulation, and target media and information programmes accordingly;

   f. Improve individuals' ability to evaluate the authenticity and origins of AI generated information and other content shared on online information platforms, for example through appropriate and

tested labelling, and to detect inauthentic behaviour by supporting and developing scientific research and technical tools to facilitate this task;

g. Put in place effective and meaningful democratic and participatory engagement mechanisms, where relevant and appropriate, around policy design and implementation related to information integrity, and assess the use of participatory democracy tools to facilitate inclusive and informed civic discussion on societal issues;

h. Create mechanisms and tools for the public to report malicious or inauthentic online activities affecting information integrity;

2. Enabling greater understanding of how information flows and promoting innovation and research by academia and civil society, through cooperation with government actors, by encouraging or requiring online information platforms, as appropriate, to:

a. Put in place information sharing mechanisms, for example between content creation platforms (including providers and deployers of AI systems), content dissemination platforms, civil society, independent fact checkers, academic partners, media and journalists, and the government to take appropriate action to respond to disinformation, as relevant and appropriate;

b. Provide greater access to public and non-public data and information by providing a dedicated data sharing infrastructure to monitor potential information integrity risks, while ensuring appropriate and sufficient privacy and personal data protection measures to prevent harmful outcomes for data subjects, including, for example, by limiting data access to independent, vetted researchers who meet specific requirements, which increase with data sensitivity, designed to ensure that research is conducted for legitimate aims and to help prevent abuse;

c. Consider creating advertising databases that are accessible and include archived advertisements, even after they have been removed, to increase transparency and oversight over where advertisements are displayed and provide greater access to advertisement details to individuals and researchers.

3. Building the public's understanding of how online information platforms operate through enhancing transparency and information sharing and co-operation between governments, online information platforms, academics, civil society actors, and users by encouraging or requiring online information platforms, as appropriate, to:

a. Provide information, and conduct and regularly publish research on the options, impact, and summary results of platform designs and algorithmic recommendation systems developed to limit the spread of disinformation (including, when appropriate, the impact of bridging-based ranking, prioritisation based on potential indicators of information integrity, latency and friction, re-share limits, and with a database of algorithmic changes), so that users are able to understand how their feeds or online experiences are tailored, while recognising the need to protect trade secrets and patents, and to prevent malign actors from using such information to further promote disinformation;

b. Publish, in accessible formats and country-appropriate languages, information about their content moderation procedures, as well as about their terms of service, community standards, and privacy and personal data protection policies to help ensure that their actions are consistent with their own guidelines and policies;

c. Provide, as feasible and appropriate and in accessible formats, information about their content moderation actions, including labelling, downranking, and content removal, about the processes that trigger enforcement, including state actor requests to take action on content;

as well as offer users appeal mechanisms and recourse within the platform for disputed content moderation actions;

d. Clarify whether content is an advertisement or funded by a state actor through adequate measures, such as the provision of information on the advertiser and, where relevant and necessary, align transparency requirements for advertising with existing legislation regulating advertisements for other types of media, including in relation to electoral advertising.

4. Mitigating the risks posed by foreign information manipulation and interference, and foreign actors' efforts to undermine democracy more widely, by, as appropriate and as deemed necessary in the national context:

a. Developing risk assessments and response strategies, as appropriate, to help frame efforts to counter foreign information manipulation and interference;

b. Consider pursuing effective, proportionate, and dissuasive sanctions against actors that are proven to manage or conduct foreign information interference operations based on an established and transparent legal basis and overseen by an independent judiciary;

c. Considering putting in place mechanisms to increase the disclosure, the denunciation, or the legal disablement of affiliations and activities that are intended to use information operations to influence the national public debate or public officials carrying out the decision-making process, such as through transparency registers for foreign influence activities providing a means for establishing whether non-registered activities constitute information operations

d. Expanding, as appropriate, information exchange mechanisms with trusted peer countries on FIMI tactics, tools, and methods, including disinformation as a service, used by hostile foreign actors and exploring how to adopt common approaches for the disclosure of FIMI campaigns.

5. Monitoring and evaluating the impact of information manipulation and policy responses to strengthen information integrity, as appropriate, in particular by taking steps to:

a. Build capabilities to regularly assess the risk and, where possible, impact of disinformation and other forms of information manipulation in the information environment , including on freedom of expression, and its evolution over time;

b. Develop frameworks for assessing the effectiveness of approaches with clear and measurable indicators for to promote information integrity and facilitate their ongoing refinement;

c. Work with a wide range of non-governmental actors to develop assessments on effectiveness of policy responses and their consequences on civic space.

Enhance the transparency, accountability, and plurality of information sources

IV. RECOMMENDS that Adherents reinforce information integrity in the creation and dissemination of information by enhancing the transparency, accountability, and plurality of information sources by:

1. Upholding independent and pluralistic journalism and public interest media as essential components of democracies and the promotion and protection of human rights, and facilitating, as appropriate, new forms of evidence-based and reliable information production and dissemination, including innovative digital reporting, in particular through:

a. Reinforcing media pluralism and an independent media sector, including public interest media and preventing news desert, for example through encouraging competition, promoting

transparency and diversity of media ownership, and encouraging editorial independence in an effort to prevent undue influence;

b. Creating and maintaining an enabling environment for journalists and media workers to carry out their work independently and without undue interference and protected from physical, psychological, and other online and off-line threats, and providing an enabling environment for independent fact checkers;

c. Reinforcing the role of journalism as essential to upholding democracy and human rights (notably local, regional, and community media in areas with low internet connectivity, media in minority languages, investigative journalism, among others), including by facilitating, as appropriate, indirect or direct financial support to news providers that contribute to the achievement of democratic objectives, applying transparent, independent, predictable, and non-discriminatory governance and oversight of such support, where applicable, to ensure independence from government; this may also include exploring innovative models for funding of independent media, such as blended finance and impact investment;

d. Supporting, where appropriate, independent and evidence-based public service media as a source of news and information, safeguarding editorial independence and institutional autonomy;

e. Providing adequate protections against Strategic Lawsuits Against Public Participation (SLAPP) and strengthening whistleblower protections and reporting mechanisms;

f. Considering how to promote dialogue between relevant stakeholders regarding remuneration models for journalistic content shared on online information platforms to help support local, pluralistic, independent, and public interest media;

g. Encouraging the disclosure of conflict-of-interest between media content and the private interests of the owner(s) of media outlets where financial, legal, or other relationships could influence reporting, as well as transparency around advertising, sponsored, and promoted content;

h. Encouraging media companies to safeguard editorial independence and to establish ethical or integrity standards on: (i) effectively managing potential conflicts between journalists' and contributors' interests connected to the content they create; (ii) accepting gifts, invitations, and hospitalities from lobbying and influence actors; (iii) dealing with external pressure from lobbying and influence actors aiming to influence coverage; (iv) and interacting with partners or funders;

i. Encouraging and assisting, as appropriate, journalists and media to understand and respond to the sources and methods of disinformation and co-ordinated inauthentic behaviour on their sites, such as the use of fake and mimicked websites (website spoofing);

j. Exploring efforts to avoid market concentration of online information platforms, particularly if it strengthens market power, and encouraging competition between them, as a means to foster information integrity;

k. Encouraging, as appropriate, the development, by industry or other non-governmental stakeholders, of voluntary standards of professional integrity related to new forms of information production and dissemination, in particular for digital content creators and other online actors who share content for financial or reputational gain, such as influencers and automated news generation platforms;

l. Promoting transparency with regards to advertisements made by digital content creators and other online actors who share content for financial gain, for example by labelling promoted posts as advertisements in a clear, legible, and identifiable manner and by clearly identifying on whose behalf the sponsored post is made;

m. Helping build the capacity of media outlets on how new technologies such as AI can be constructively and responsibly leveraged in the newsrooms;

n. Reflect on the spread of disinformation by firms and other actors using co-ordinated inauthentic behaviour for profit and the ways to best address the issue.

2. Strengthening co-operation between civil society, academics, industry, and governments, and reinforcing the conditions for trust in online information platforms' systems and processes by encouraging or requiring online information platforms, as appropriate, to:

a. Adopt a human rights-respecting approach and employ business practices that contribute to information integrity;

b. Enable users to report accounts or content that may violate national laws, other applicable laws, or the terms of services of the platform by developing and putting in place easily accessible reporting tools or mechanisms;

c. Provide users with greater flexibility to control their experiences on platforms based on their preferences (including, for example, by turning off personalisation algorithms or limiting the content they see only to that which is generated by selected contacts); as well as, as appropriate, identify opportunities to open platforms' Application Programming Interface (API) to encourage development of third-party tools, software, and services (known as "middleware") to enable users to tailor experiences to their needs and interests and introduce competition and innovation into markets;

d. Appropriately resource their content moderation systems and their human resources, including by setting up teams that are: proportional to the number of users and languages in the jurisdiction in which they operate; responsive to specific risks and key political events such as elections; knowledgeable of local languages and national and international legal requirements, including, but not limited to, legal requirements pertaining to freedom of expression; and able to collaborate with independent fact-checkers and trusted flaggers to address the spread of disinformation in a timely manner (for example, through policies on content removal, downranking, increasing latency, friction, and imposing re-share limits, as well as introducing bridging-based ranking, prioritisation based on potential indicators of information integrity, and providing context for users);

e. Designate accessible representatives, resourced proportionally to the number of platform users in the country or jurisdiction in which they operate, to enable the exchange of timely and contextualised information and to provide an effective channel for dialogue between online information platforms, regulators and government liaisons;

f. Designate a legal representative responsible for the country or jurisdiction in which the online information platform operates, as appropriate;

g. Establish or reinforce their early warning and response systems, adapted to country contexts, which enable timely provision of reliable public interest information during crises and military conflicts when mis- and disinformation can have particularly damaging consequences;

h. Establish or reinforce mechanisms to engage with local and trusted third-party stakeholders to help provide accessible, timely, and reliable information in contexts of crisis and conflict;

i. Put in place mechanisms to detect and respond to incidents involving the creation and dissemination of technology-facilitated gender-based violence, image-based abuse, deepfake pornography and disinformation designed to obstruct or prevent individuals from exercising the right to vote;

j. Encourage reducing financial incentives for the spread of mis- and disinformation by giving purchasers of online advertising information on, and oversight over, where their advertisements are placed to avoid inadvertently supporting actors spreading disinformation;

3. Building trust in the information ecosystem and increasing multi-stakeholder co-operation by encouraging or requiring online information platforms, as appropriate, to:

a. Prevent the spread of disinformation, for example by banning the use of bots when they are used by malicious actors, including private actors, on large platforms to deceive the public or to undermine electoral processes or human rights;

b. Identify and label bots and inauthentic accounts to mitigate the risks posed by co-ordinated inauthentic behaviour;

c. Collaborate with providers and deployers of AI systems to authenticate and clarify provenance of AI-generated content, and commit to using available industry standards that display easily traceable markers, particularly but not only used in electoral processes, to the extent technically feasible and appropriate;

d. Minimise the risk of harm from misinformation, disinformation and other forms of information manipulation, technology-facilitated gender-based violence, image-based abuse, and deepfake pornography on online information platforms by thoroughly evaluating the risk levels associated with their products and services;

e. Create and publish a public version of risk assessments focused on issues related to information integrity. This could, include on risks related to the training and use of AI tools and those posed to human rights, taking care to ensure that malicious actors are not able to benefit from the release of information related to digital platform responses;

f. Engage with independent actors to continue to develop, conduct and publish a comprehensive public version of independent audits or reviews on online information platforms' risk assessments following clearly defined standards.

4. Helping ensure children can thrive in an environment conducive to the full exercise of their right to freedom of opinion and expression, their future ability to participate in the democratic process, and that does not encourage problematic or excessive use of digital technologies, by encouraging or requiring online information platforms, as appropriate depending on children's age, to:

a. Consider restricting advertisements targeted to children, based on profiling data;

b. Consider measures that ensure the privacy, personal data protection, safety, and security of children on their services, such as controls to provide parents or guardians the ability to manage children's activities online, child-friendly complaints and reporting systems, children-safe flagging systems, enhanced digital identity protections, and tools designed to help signal abuse or access support;

c. Reflect with government and civil society on initiatives and voluntary efforts from online information platforms to promote children's appropriate use of online information platforms; reflect on the merits of stricter limitations on children's access to and use of online information platforms, through, for example and as appropriate, establishing minimum age requirements for the use of platforms without parental consent; developing and applying age verification tools

to limit platform access, recognising the need for safeguards to respect individuals' privacy, personal data protection, and maintain equitable access to an open and free internet; and labelling risks to children.

Upgrade institutional architecture and open government practices

V. RECOMMENDS that Adherents upgrade their institutional architecture to strengthen information integrity, while reinforcing transparency and checks and balances on governments' actions in this field, taking into account open government principles, by:

1. Establishing transparency and public reporting requirements for government requests to trace, limit, block, or remove content or users on online information platforms in a manner that ensures appropriate and sufficient privacy, personal data, national security, and law enforcement protection measures.

2. Developing transparent processes and related guidance for public officials, as appropriate, that:

   a. Clarifies their responsibilities and increases transparency related to government requests to trace, limit, block, or remove content on online information platforms as well as the number of requests made;

   b. Clarifies their responsibilities related to authentication and provenance of AI-generated content produced or published by government officials in order to facilitate the identification of content generated or meaningfully altered with AI systems;

   c. Clarifies their responsibilities related to interactions with civil society, academia, and online information platforms on information integrity issues, as well as outlines the appropriate channels and responsible government counterparts, review processes, and procedures to help clarify mandates, avoid undue pressure on freedom of expression, and ensure clarity and predictability of government engagement with non-governmental actors.

3. Supporting a coherent vision and a comprehensive approach to reinforcing information integrity and upholding universal human rights by developing and implementing strategic frameworks or guidance that:

   a. Focus specifically on information integrity and tackling misinformation, disinformation, and other forms of information manipulation, or include responding to disinformation and building information integrity in other official documents such as strategies on digitalisation, democracy, trust, national security, public communication, or education;

   b. Describe objectives, time frame, scope, and operational aspects around the institutional setting, reporting, and evaluation processes of relevant strategies and guideline documents;

   c. Enable monitoring of implementation by collecting credible and relevant evidence of the frameworks' implementation and providing recommendations for their improvement, with particular attention paid to upholding human rights and fundamental freedoms.

4. Providing clear and transparent mandates to the relevant agencies, offices, units, or co-ordination mechanisms, in particular through taking steps to:

   a. Outline or clarify the function and objectives of relevant offices, units, or co-ordination mechanisms to define the mandate and the parameters within which they operate, and, if relevant, to put in place governance mechanisms to ensure the institutions responsible for detecting and responding to misinformation, disinformation, and other forms of information manipulation have appropriate and transparent institutional checks and balances;

b. Connect sectoral priorities, enable prompt information-sharing, taking into account potential limitations in sharing classified information and personal data , and avoid duplication of efforts between institutional authorities within governments through, for example, the creation of task forces that provide technical advice on policies related to specific cross-cutting issues, such as AI, foreign interference, and electoral interference;

c. Define internal governance mechanisms with appropriate checks and balances to enable timely and effective responses to information integrity risks during crises, including, as appropriate, dialogue mechanisms with online information platforms, other private sector actors, and civil society.

d. Clarify whether and how independent regulatory mechanisms and governance may be developed to ensure enforcement and compliance by online information platforms, such as through a newly established regulator or through strengthening existing regulators, as appropriate, and to provide the regulator(s) with a mandate to, for example: receive and evaluate disclosure reports and risk assessments from online information platforms; investigate and monitor online information platform compliance with applicable legislation; impose sanctions on online information platforms for non-compliance; and issue recommendations to help online information platforms adapt their practices; or, as appropriate, encourage online information platforms to develop self- or co-regulatory frameworks to address aspects not falling under the scope of the regulatory framework.

5. Deterring and mitigating the specific risks to electoral processes and maintaining a safe and enabling environment that is conducive to the exercise of citizens' right to participate in public affairs through independent electoral management bodies and other offices, as appropriate, by:

a. Providing timely and reliable information on electoral processes to enable citizens to exercise their rights, with a focus on ensuring information is accessible to persons and groups who may be in vulnerable situations, including communities with limited access to technology;

b. Strengthening election-related cybersecurity mechanisms and efforts to share information on specific disinformation threats and strengthening co-operation on election-related matters with other offices with relevant competence;

c. Countering or prohibiting the spread of false or misleading information that is designed and disseminated with the intent to obstruct or prevent citizens from exercising the right to vote, or to disrupt the election process, including but not limited to false or misleading information concerning the time, place, or manner of holding an election, the qualifications for or restrictions on voter eligibility, and threats to physical safety associated with casting a ballot, through measures that are proportional to the risks and uphold human rights;

d. Protecting the safety of electoral workers by countering or prohibiting the spread of false information that is disseminated with the intent to harass or intimidate electoral workers;

e. Countering or prohibiting the use of malicious AI-generated content, such as deepfakes, that pose specific and well-defined risks to electoral processes;

f. Publishing – in the case of independent electoral management bodies – electoral strategies that provide information on the relevant government agencies and the processes used to administer elections to build trust in electoral management bodies.

6. Enhancing international co-operation to strengthen the collective response to challenges to information integrity, in particular through efforts to, as appropriate:

a. Create and expand partnerships, networks, and cooperative mechanisms to connect actors across sectors and countries to share information, experiences, analytical methodologies, as well as public policy responses and their results;

b. Develop knowledge sharing processes and practices for governments to responsibly communicate information about content provenance and synthetic content;

c. Support countries, where relevant and appropriate, in efforts to reinforce local, pluralistic, independent, and public interest media through official development assistance and media development agencies;

d. Increase the levels of financial and other forms of assistance and to improve the relevance and effectiveness of existing support to preserve, protect, and promote public interest media and information integrity.

e. Enhance bilateral and multilateral cooperation programs on research and innovation regarding the support of information integrity.

7. Providing capacity-building and sufficient resources at the local, national, and international level, where possible and appropriate, for public officials who analyse and respond to disinformation and other information manipulation threats, through efforts to:

a. Provide adapted training and upskilling at all levels of government and ensure that adequate resources (human, technical, and financial) are in place to effectively detect, monitor, and counter the spread of information manipulation without impinging on freedom of opinion and expression;

b. Systematically apply public management tools such as strategic foresight and regulatory impact assessments to improve decision making and planning capacity to anticipate how rapid and uncertain technological and social changes in the information environment will affect democratic engagement;

c. Develop, to the degree possible, government institutions' abilities to use AI technologies and tools for strengthening information integrity, including related to identifying artificial amplification activities and synthetic content detection systems.

8. Developing, adopting, and implementing initiatives to promote open government, including through an enhanced public communication function, by:

a. Clarifying the role and building the capacity of the public communication function to deliver understandable, accessible, relevant, timely, trustworthy (i.e. transparent, accurate, and comprehensive) information to the public;

b. Deploying, where possible, content provenance systems to establish and verify the authenticity and provenance of government-produced content;

c. Lowering barriers for journalists and citizens to access public information and official data, as needed and required, that is easy to understand, verifiable, and following accessible formats in the digital environment;

d. Upholding or updating, as needed and required, access to information laws, open government and data standards;

VI. **ENCOURAGES** relevant stakeholders to promote and follow this Recommendation;

VII. **INVITES** the Secretary-General and Adherents to disseminate the Recommendation.

VIII. **INVITES** non-Adherents to take account of and adhere to the Recommendation.

IX. **INSTRUCTS** the Public Governance Committee, in consultation with other relevant committees, to:

a. Serve as a forum for exchanging information on strengthening information integrity including experience with the implementation of this Recommendation, and to foster multi-stakeholder and interdisciplinary dialogue to build understanding of relevant and effective policy responses in this space;

b. Develop practical guidance and indicators to support the implementation of this Recommendation;

c. Update Council on the progress made in supporting the implementation and dissemination of this Recommendation no later than two years after its adoption; and

d. Report to the Council on the implementation, dissemination, and continued relevance of this Recommendation every five years following its adoption.

***