Recommendation of the Council on Information Integrity

OECD Legal Instruments

OECD

BETTER POLICIES FOR BETTER LIVES

This document is published under the responsibility of the Secretary-General of the OECD. It reproduces an OECD Legal Instrument and may contain additional material. The opinions expressed and arguments employed in the additional material do not necessarily reflect the official views of OECD Member countries.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

For access to the official and up-to-date texts of OECD Legal Instruments, as well as other related information, please consult the Compendium of OECD Legal Instruments at http://legalinstruments.oecd.org.

Please cite this document as:
OECD, *Recommendation of the Council on Information Integrity*, OECD/LEGAL/0505

Series: OECD Legal Instruments

Photo credit: © Shutterstock/Rawpixel.com

© OECD 2025

This document is provided free of charge. It may be reproduced and distributed free of charge without requiring any further permissions, as long as it is not altered in any way. It may not be sold.

This document is available in the two OECD official languages (English and French). It may be translated into other languages, as long as the translation is labelled "unofficial translation" and includes the following disclaimer: *"This translation has been prepared by [NAME OF TRANSLATION AUTHOR] for informational purpose only and its accuracy cannot be guaranteed by the OECD. The only official versions are the English and French texts available on the OECD website http://legalinstruments.oecd.org"*

Background Information

The Recommendation on Information Integrity was adopted by the OECD Council on 17 December 2024 on the proposal of the Public Governance Committee (PGC). The Recommendation aims to establish a wide-ranging and applicable policy framework for Adherents to address threats posed by information manipulation and to put in place measures that promote information integrity in line with the universal human rights of freedom of opinion and expression.

The need for a standard on information integrity

The digital transformation of societies has reshaped how people interact and engage with information. Advancements in digital technologies and novel forms of communication have changed the way information is produced, shared, and consumed, locally and globally and across all media. Technological changes and the critical importance of online information platforms offer unprecedented access to information, foster citizen engagement and connection, and allow for innovative news reporting. However, they can also provide a fertile ground for the rapid spread of false, altered, or misleading content. In addition, new generative AI tools have greatly reduced the barriers to creating and spreading content.

Promoting the availability and free flow of high-quality, evidence-based information is key to upholding individuals' ability to seek and receive information and ideas of all kinds and to safeguarding freedom of opinion and expression.

The volume of content to which citizens are exposed can obscure and saturate public debates and help widen societal divisions. In this context, the quality of civic discourse declines as evidence-based information, which helps people make sense of their social environment, becomes harder to find. This reality has acted as a catalyst for governments to explore more closely the roles they can play, keeping as a priority in our democracies the necessity that governments should not exercise control of the information ecosystem and that, on the contrary, they support an environment where a plurality of information sources, views, and opinions can thrive.

Process for developing the Recommendation

Recognising the need to develop their policy response in the field of information integrity, Ministers and representatives from all OECD Members and the European Union, as well as Bulgaria, Croatia, Peru, and Romania, committed to address mis- and disinformation while protecting freedom of speech in the Declaration on Building Trust and Reinforcing Democracy [OECD/LEGAL/0484], adopted at the 2022 PGC meeting at Ministerial level, and the Action Plan on Public Governance for Combatting Mis- and Dis-information approved by the PGC on 5 October 2022 and welcomed in the Declaration.

The development of the Recommendation built on a multi-year process of research, analysis, and events and involved consultations both within and outside the OECD, including with the Digital Policy Committee, the Competition Committee, the Development Assistance Committee, the Education Policy Committee, the Employment, Labor, and Social Affairs Committee, and the Health Committee, as well as through a public consultation. The Recommendation also complements other existing national and international standards aimed at guaranteeing press freedom and universal human rights, including freedom of opinion and expression. To finalise the draft, multiple rounds of comments were held on the draft text in the PGC and its informal Expert Group on Governance Responses to Mis- and Disinformation.

Scope of the instrument

Building on the detailed policy framework outlined in the OECD report Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity, the Recommendation provides an ambitious and actionable international standard that will help governments develop a systemic approach to foster information integrity, relying on a multi-stakeholder approach. It provides guidance for policymakers in democratic governments under three mutually reinforcing building blocks, which together recommend that Adherents:

i. “Strengthen societal resilience” through promoting media literacy and critical thinking skills to provide individuals the capacity and knowledge to navigate the information environment effectively and responsibly, as well as through working with actors across society to develop greater understanding of the evolution of the information landscape and promoting innovation and research;

ii. “Enhance the transparency, accountability, and plurality of information sources” by focusing on the role played by digital platforms and traditional media and journalists; and

ii. “Upgrade institutional architecture and open government practices” by providing strategic guidance, clear and transparent mandates, and capacity building and sufficient resources to upgrade governmental institutions to respond effectively.

Next steps

The PGC will support the exchange of information and experience to facilitate the implementation of this Recommendation, through a multi-stakeholder and interdisciplinary dialogue. With the support of its Hub on Information Integrity, the PGC will monitor activities, good practices, and emerging trends around information integrity through relevant data collection, analysis, and dissemination of results, and develop guidance and tools to support the implementation of this Recommendation.

The PGC will update Council on the progress made in supporting the implementation and dissemination of this Recommendation no later than two years after its adoption, and will report to the Council on the implementation, dissemination, and continued relevance of this Recommendation at least every five years following its adoption.

For further information please consult: https://www.oecd.org/en/topics/sub-issues/disinformation-and-misinformation.html.
Contact information: pgccontact@oecd.org.

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, regulatory policy and governance (including agile regulatory governance to harness innovation), 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 and should be lawful, justified, proportionate, respecting human rights laws and obligations;

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, trust in institutions, and public discourse, and posing a fundamental risk for democracies and universal human rights;

RECOGNISING that public policies can be 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, and that these policies should enhance and not undermine, essential safeguards for democracies, including media pluralism, laws that protect freedom of opinion and of expression, privacy, 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 access to high-quality and public interest media and journalism plays a critical role in democracies and for information integrity;

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 ubiquitous, high-quality and affordable 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 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 unduly 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 engage in 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 environment, 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, implement, and evaluate 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, including by protecting the independence and integrity of research in this domain;

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 can have negative implications for information integrity and human rights through the potential for faster, wider, and more targeted dissemination of disinformation, and that these challenges call for a continued focus on the development of effective standards in this space aimed at guaranteeing human rights;

RECOGNISING that new and emerging technologies, including advanced artificial intelligence (AI) systems, in particular generative AI, continue to present new and evolving opportunities and risks for information integrity, and that new technologies, including AI, can be used in the fight against disinformation, as well as a means to create and disseminate disinformation faster, less expensively, and more easily;

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 increasing transparency and establishing clear guidelines for governments regarding interactions with online information platforms and other actors of the information environment is important for maintaining public trust and ensuring accountability of democratic institutions;

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 public policies and tools to reinforce information integrity in the evolving digital environment will need continuous evaluation and adjustment.

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 also respecting 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 with 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, or 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 environment 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 plural and diverse 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 a set of skills and competencies that enable citizens to critically, effectively, and responsibly access, understand, use, and engage with information and media, both online and off-line; this can include digital literacy, news literacy, media literacy, algorithm literacy, and AI literacy.
- **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.
- **Online information platforms** refer to digital services that also collect, store and disseminate information to users, often at the user's request, through public or semi-public channels, including, for example, search engines, social media platforms, message boards, app ecosystems, online forums, and gaming and virtual worlds, where information sharing and curation are central to their operations.
- **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 legal actions that are threatened, initiated or pursued as a means of harassing or intimidating their target, and which seek to prevent, inhibit, restrict or penalise free expression on matters of public interest and the exercise of rights associated with public participation.

Strengthen societal resilience

III. RECOMMENDS that Adherents strengthen societal resilience to misinformation, disinformation, 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, teachers, libraries, cultural institutions, civil society organisations, journalists, media outlets, 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 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 harness opportunities and 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. Integrate, include, or promote media and information literacy in school curricula, according to children's developmental stage, from early childhood education to higher education; develop training programmes for teachers; and promote media and information literacy in adult learning and lifelong education;

   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 build understanding and societal resilience, as well as provide reliable information on threats to the public, platforms, researchers, journalists, 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 adapt media and information literacy 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, hashing, watermarking, or other content provenance measures, 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;

i. Encourage reflection on the spread of disinformation and other forms of information manipulation by firms and other actors using co-ordinated inauthentic behaviour for profit, as well as on the ways to best address the issue.

2. Enabling greater understanding of how information flows and promoting innovation and research by academia and civil society, including through cooperation with government actors when appropriate, 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 and other forms of information manipulation, 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 data protection measures to prevent harmful outcomes for data subjects, including, for example, by limiting data access to independent researchers, civil society organisations, and journalists who meet specific requirements that ensure appropriate handling related to user privacy, security, and proprietary considerations and 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 and other forms of information manipulation (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 the abuse of such information by malign actors;

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 and their respective change over time 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 FIMI, 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. Considering the pursuit of 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, following due process and overseen by an independent judiciary;

c. Considering putting in place mechanisms to increase the disclosure or the legal disablement of affiliations and activities that are intended to conduct foreign information manipulation and interference operations targeting 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 disinformation and other forms of information manipulation, as well as 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 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 public 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, public interest media, and press freedom 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 deserts, 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, media workers, and independent fact-checkers to carry out their work independently and without undue interference, including through protections from physical, psychological, and other online and off-line threats and protections related to the confidentiality of their sources;

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 public service media as a source of evidence-based 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 the feasibility of remuneration models for journalistic content shared on online information platforms to help support local, pluralistic, independent, and public interest media, taking into account the value of such journalistic content to online information platforms and the value provided by online information platforms to public interest media;

g. Encouraging the disclosure of conflict-of-interest between media content and the private interests of the direct owner(s) or beneficiaries 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 or content they create; (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 and furthering fairness of the broader online information platform ecosystem for firms and users, 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; as well as voluntary standards of professional integrity for new forms of verification and fact-checking.

l. Promoting transparency with regards to advertisements made by digital content creators and other online actors who share content for financial gain, such as influencers and automated news generation platforms, 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 and encouraging the development of ethical guidelines for the use of AI-based technologies in journalism;

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 and other applicable laws, or the terms of service 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 and other forms of information manipulation 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 is established or 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 and other forms of information manipulation can have particularly damaging consequences;

h. Establish or reinforce mechanisms to engage with local and trusted third-party stakeholders, including public interest media and journalists, 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 and other forms of information manipulation designed to obstruct or prevent individuals from exercising the right to vote;

j. Encourage reducing financial incentives for the spread of disinformation, including 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 environment and increasing multi-stakeholder co-operation by encouraging or requiring online information platforms, as appropriate, to:

a. Prevent the spread of co-ordinated inauthentic behaviour, for example by banning the use of bots when they are used by malicious actors, including private actors, on online information 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 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 and responding to the risk levels associated with the design, promotion, and deployment of their products and services;

e. Create and publish a public version of risk assessments focused on issues related to information integrity, which could include a focus on risks related to the design, training and use of AI tools and those posed to human rights;

f. Engage with independent actors to continue to develop, conduct and publish a comprehensive public and accessible 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, 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, civil society, expert communities, parents and families on initiatives and voluntary efforts from online information platforms to promote children's appropriate use of online information platforms and 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; labelling risks to children; and recognising the need for safeguards to respect individuals' privacy and security while maintaining equitable access to an open and free internet and upholding children's right to freedom of opinion and expression.

Upgrade institutional architecture and open government practices

V. RECOMMENDS that Adherents develop and 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, 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 restrictions 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 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 (short-medium and long-term targets), 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 transparent 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 private data of individuals, 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 undertaking a consistent and long-term approach to 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 information threats and strengthening inter-agency co-operation on election-related matters;

c. Countering or prohibiting the spread of disinformation and other forms of information manipulation 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 disinformation and other forms of information manipulation 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. 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, multilateral, and multi-stakeholder co-operation 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 forms of information manipulation, 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 disinformation and other forms 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 at least every five years following its adoption.

About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Legal Instruments

Since the creation of the OECD in 1961, around 460 substantive legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions** are adopted by Council and are legally binding on all Members except those which abstain at the time of adoption. They set out specific rights and obligations and may contain monitoring mechanisms.

- **Recommendations** are adopted by Council and are not legally binding. They represent a political commitment to the principles they contain and entail an expectation that Adherents will do their best to implement them.

- **Substantive Outcome Documents** are adopted by the individual listed Adherents rather than by an OECD body, as the outcome of a ministerial, high-level or other meeting within the framework of the Organisation. They usually set general principles or long-term goals and have a solemn character.

- **International Agreements** are negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangement, Understanding and Others**: several other types of substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.