



**MEMORANDUM OF UNDERSTANDING BETWEEN
THE GOVERNMENT OF THE UNITED KINGDOM
AND
THE GOVERNMENT OF AUSTRALIA
CONCERNING ONLINE SAFETY AND SECURITY**

Summary

1. The Government of the United Kingdom of Great Britain and Northern Ireland ("the United Kingdom"), as represented by the Department for Science, Innovation and Technology, and the Government of Australia, as represented by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, (hereafter "both Participants") have decided to establish a forward looking and comprehensive online safety and security memorandum of understanding.
2. The UK-Australia Online Safety and Security Memorandum of Understanding (hereafter "this MoU"), builds on the existing deep and historic partnership between both Participants, including the Australia-UK Ministerial Consultations (AUKMIN) and the UK-Australia Cyber and Critical Technology Partnership.
3. This MoU will serve as a strategic framework for both Participants to jointly deliver concrete and coordinated online safety and security policy initiatives and outcomes to support their citizens, businesses and economies.
4. The initial focus and scope of this MoU will be on the following policy areas: harmful online behaviour, age assurance, safety by design, online platforms, child safety, technology-facilitated gender-based violence, safety technology, online media and digital literacy, user privacy and freedom of expression, online child sexual exploitation and abuse, terrorist and violent extremist content, lawful access to data, encryption, misinformation and disinformation, countering foreign interference, online scams/fraud, information sharing around regulation, and the impact of new, emerging and rapidly evolving technologies (such as Artificial Intelligence (AI) – including machine learning and generative AI models) in these areas.

Background

5. Both Participants share a common approach to protecting people from harms that are digital in nature or are facilitated by technology, including the importance of safe, secure and privacy preserving online environments, and the need for government and industry to proactively mitigate harms, now and as technology develops.
6. Both Participants share fundamental values, including freedom of expression, human rights, democracy and the rule of law and are committed to shaping a global

consensus on tackling online harms and collaborating on a range of issues relating to online safety and security (as outlined in paragraph 4), through modalities such as in-person dialogues, coordinated bilateral and multilateral engagement, and regulatory engagement. Both Participants acknowledge previous initiatives as well as work already underway by both Participants to align our interests.

Strategic objectives

7. Under this MoU, both Participants will take a comprehensive approach to online safety and security, recognising the economic, social and individual benefits that stem from a safe and secure online environment. This MoU will also contribute to mitigating the risks of harm in a rapidly-developing technological landscape – ensuring the protection of the public by reducing long-standing and novel causes of harm, in particular the harms experienced by children, women and other persons or groups in vulnerable situations, while maintaining capabilities in a way that protects privacy, and does not limit freedom of expression or stifle innovation.

Joint actions

8. **Global thought leadership and international engagement.** Both Participants will seek to coordinate engagement with international partners to champion collaborative approaches to online safety and security, helping to contribute to the objectives of this MoU. Both Participants will endeavour to make effective use of their differing geographies and memberships of regional and international groupings to promote an approach to online safety that champions their joint commitment to an open, free, safe and secure internet that all users can benefit from.
9. **Regulation and enforcement.** Both Participants' respective regulatory frameworks provide scope for sharing of information, intelligence and best practice - and for deepened collaboration and investigatory cooperation. Both Participants support regulatory coherence and increased coordination between independent regulators at an international level. Both Participants will also seek to increase cooperation between their respective law enforcement agencies and regulators to enhance their respective detection, investigative, disruption and enforcement capabilities, including identifying opportunities to collaborate on technical solutions.
10. **Online safety and security principles.** Both Participants will seek to play a key role in the shaping and promotion of consistent principles and approaches for online safety – including on issues such as the use of age assurance technologies, age-appropriate design, and safety by design principles and practices – building on strong existing cooperation with wider international partners and multi-stakeholder groups.
11. Both Participants will seek to amplify existing specifications, procedures, guidelines, standards and principles, and facilitate effective cooperation internationally to ensure safety, privacy and security are built in by design for new and emerging technologies

(including AI), advocating an approach that promotes and protects human rights online.

12. **Tech industry accountability.** Both Participants will seek to coordinate engagement with global technology companies on issues of mutual interest to help ensure safety is built into the design, development and deployment of online platforms, services, systems and products
13. Both Participants will work together to help develop common positions among like-minded partners and enhance collaboration between industry and governments to address challenges posed by design choices, and to ensure end-to-end encryption and technologies that aim to enhance privacy and security do not undermine the right to safety, especially for children, and tightly controlled lawful access to data. Both participants will continue to advocate and encourage industry adoption of existing international transparency frameworks.
14. **Countering misinformation and disinformation.** Both Participants will share best practice and deepen collaboration on countering misinformation and disinformation – a threat to our democracies and social cohesion. Both Participants will seek to pursue a programme of targeted joint capacity building and strategic engagement with technology platforms and strengthen the impact of relevant international fora on misinformation and disinformation.
15. **Countering foreign interference.** Both Participants will share best practice and deepen collaboration of responses to foreign interference, particularly foreign information manipulation and interference activities that threaten democracy, and community interference (transnational repression). Both Participants will leverage new and existing forums, as well as strengthening our strong bilateral relationship, to pursue a programme of knowledge sharing, and to develop tangible policy responses to shared problems.
16. **Safety technology.** Both Participants will seek to stimulate the growth and promotion of an innovative, resilient and trusted international safety technology sector through policy interventions which support more efficient routes to market for safety technology solutions and innovations. Both Participants will seek to share evidence on technologies that can protect safety and trust in information online, especially where this is challenged by emerging technologies such as AI.
17. **Online media and digital literacy** (*including online safety education*). Both Participants recognise the importance of empowering and educating their citizens to make safe and informed choices online. Both Participants will develop and promote evidence-based online media and digital literacy initiatives for all user groups, particularly under-served communities and groups most at-risk of harm, in response to online harms, including misinformation and disinformation.

Governance

18. This MoU will establish a new annual online safety and security policy dialogue to review strategic progress under the MoU, including helping to set future priorities and areas of cooperation.
19. This will be complemented by suitable arrangements for governance and practical discussion of individual topics and policy areas.
20. Both Participants will engage with industry, academia and civil society groups as necessary to ensure the outputs and outcomes of this MoU deliver for all sections of society.
21. In the implementation of this MoU, both Participants will maintain high security standards and robust governance arrangements for the handling and processing of sensitive information.
22. The scope, objectives and nature of cooperation will be reviewed in response to domestic and international developments and priorities.

Administration

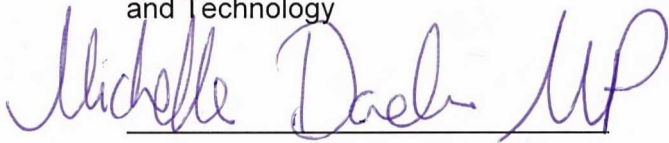
23. This MoU may be amended at any time by the mutual written consent of both Participants.
24. This MoU may be terminated by either Participant giving at least six month's written notice to the other Participant. The Participants will consult to determine how any outstanding matters should be dealt with.
25. Any disputes about the interpretation or application of the MoU will be resolved by consultations between the Participants, and will not be referred to any national or international tribunal or third party for settlement.
26. This MoU will come into effect on the date it has been signed on behalf of the Participants and will remain in effect until terminated in accordance with Paragraph 24.
27. This MoU represents the understanding reached between the Participants and does not create any legally binding rights or obligations. Nothing in this MoU will alter or affect any existing agreements between the Participants. Both Participants acknowledge that this MoU will not be deemed as an international agreement and will not constitute or create legal obligations governed by international law.

Signatories

Signed in London, UK on 20 February 2024.

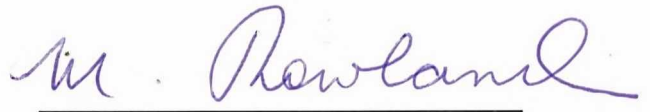
For the Government of the United Kingdom

The Rt Hon Michelle Donelan MP
Secretary of State for Science Innovation
and Technology

A handwritten signature in purple ink, reading "Michelle Donelan MP", written over a horizontal line.

For the Government of Australia

The Hon Michelle Rowland MP
Minister for Communications

A handwritten signature in purple ink, reading "M. Rowland", written over a horizontal line.