

Submission to the Department of Social Services ICMEC Australia

Consultation on the Second Action Plan under the National Plan to End Violence against Women and Children 2022–2032

1. About ICMEC Australia

The International Centre for Missing and Exploited Children (ICMEC) Australia works to prevent and respond to child sexual exploitation and abuse, including online child sexual exploitation and abuse (OCSEA). ICMEC Australia engages with government, industry, law enforcement, and civil society – including through the SaferAI for Children Coalition – to advocate for evidence-based, child-centred policy and regulation of technology.

While ICMEC Australia's primary mandate is child protection, we recognise that child sexual exploitation and abuse does not occur in isolation from other forms of gender-based violence. ICMEC Australia's work consistently shows that the technologies and regulatory gaps enabling child exploitation intersect with the conditions driving violence against women, underscoring the need for coordinated action across both sectors. ICMEC Australia welcomes the opportunity to contribute to the Second Action Plan consultation and offers the following perspectives from the child protection and online safety sector.

2. Executive summary

ICMEC Australia supports the National Plan's ambition to end violence against women and children in a generation. The Second Action Plan offers a critical opportunity to ensure the framework keeps pace with rapidly evolving technology-facilitated harms, particularly those affecting children and young people, and to strengthen the system coordination and law enforcement capability needed to prevent and respond to these harms effectively.

Our submission focuses on three priority areas where ICMEC Australia has specific expertise: technology-facilitated harm and the regulatory response; prevention through law enforcement capability and digital engagement; and system coordination across the child protection and gender-based violence sectors.

3. Summary of recommendations

1. Introduce a dedicated criminal offence for the creation, supply and distribution of AI 'nudification' tools and non-consensual deepfake sexual imagery, complementing existing regulatory measures and the government's Sep 2025 announcement to ban nudify apps.
2. Expand the eSafety Commissioner's authorisation environment and prevention-focused powers, consistent with the 2024 Rickard review, including a digital duty of care for online services.
3. Require AI platforms and conversational AI services to integrate referral pathways to accredited intervention services where user disclosures indicate risk of offending or harmful sexual behaviour.
4. Establish nationally consistent, trauma-informed training for all law enforcement personnel on receiving and responding to disclosures of child sexual exploitation, abuse and AI-facilitated harm.
5. Investigate and support a digital covert patrol capability for Australian law enforcement, drawing on international models such as the Danish Police's dedicated online engagement unit.

4. ICMEC Australia's position

4.1 Technology-facilitated harm: closing the legislative gap on AI tools

The rapid proliferation of AI-powered 'nudify' applications – which can generate non-consensual sexualised images of adults and children from a single photograph – represents an urgent and under-addressed harm. These tools are widely accessible, often free, and are being used to exploit both children and women. The harm occurs not only when imagery is shared, but at the point where these technologies are made available.

Existing regulatory frameworks can require platforms to restrict access to these tools, but criminal law plays an equally important role in deterring their creation, distribution and use. The United Kingdom has recently strengthened its response by criminalising the creation of sexually explicit deepfake images without consent and moving to prohibit the supply of AI nudification tools. In Australia, Independent MP Kate Chaney has similarly advocated for legislative reform – including criminalising technologies designed to generate child sexual abuse material and targeting nudify applications that facilitate exploitation. These developments reflect a growing international consensus that AI tools purpose-built for sexual exploitation should attract criminal liability.

ICMEC Australia recommends the Second Action Plan include a commitment to introduce a dedicated criminal offence for the creation, supply and distribution of nudification tools and non-consensual deepfake sexual imagery – applicable to harms against both women and children – as a necessary complement to broader online safety and platform regulation.

4.2 Prevention: expanding eSafety's powers and embedding AI referral pathways

ICMEC Australia supports expanding the eSafety Commissioner's authorisation environment and intervention capabilities to enable earlier action before harm occurs. Consistent with the Rickard review of the Online Safety Act 2021, reforms should continue the shift from reactive content removal toward a systemic, prevention-focused framework underpinned by a digital duty of care that requires online services to actively identify and mitigate risks to women and children.

A stronger prevention approach should also engage with the changing reality of how young people seek help. Research from the University of Adelaide's Australian Cybercrime Observatory, released in July 2026, found that young people are increasingly turning to AI systems for disclosure and help-seeking – often in preference to traditional authorities or support services. At least 18.7% of victims disclosed online sexual victimisation to an AI chatbot, compared with 13.2% who told a teacher, doctor, counsellor, police officer or helpline. More than a third told no person at all.

This finding highlights a significant and underutilised opportunity for early intervention. ICMEC Australia recommends the Second Action Plan include a commitment to establish a framework requiring AI platforms and conversational AI services to integrate referral pathways to accredited intervention services – including Jesuit Social Services' Stop It Now! Australia and What's OK programs – where user disclosures indicate a risk of offending, harmful sexual behaviour, problematic pornography use, or sexual thoughts involving children. Embedding referral mechanisms within AI platforms would transform AI from a passive technology into an active participant in prevention, connecting individuals to appropriate support at the earliest possible opportunity.

4.3 Law enforcement capability: training and digital engagement

Effective response to technology-facilitated violence against women and children depends critically on a law enforcement workforce that is equipped to recognise and respond to disclosures of harm. ICMEC Australia recommends the Second Action Plan include a commitment to nationally consistent, trauma-informed training for all law enforcement personnel – not only specialist units – on receiving and responding to disclosures of child sexual exploitation, abuse and AI-facilitated harm. Many victims first disclose to frontline officers, general duties police or local investigators; training must therefore be embedded across all policing jurisdictions and ranks.

The Second Action Plan should also explore a digital covert patrol capability for Australian law enforcement. The Danish Police's dedicated online patrol unit – which actively engages in gaming platforms, Discord communities, Twitch streams and other online spaces – provides a compelling model.

By 2024, the online patrol unit had generated hundreds of investigative referrals through online engagement activities, while also building trust with young people in digital-native communities. This example demonstrates the importance of these capabilities to both deter offending and improve the visibility of law enforcement in the spaces where children and young people are most at risk.

4. Conclusion

ICMEC Australia supports the Second Action Plan as an opportunity to ensure Australia's response to violence against women and children keeps pace with the rapidly evolving technology landscape. The reforms we have outlined – on AI tools, facial recognition for victim identification, expanded eSafety powers, AI referral pathways, law enforcement training, and digital engagement – are practical, evidence-based, and achievable within the timeframe of the Second Action Plan. To help ensure these reforms translate into measurable outcomes, we recommend the Second Action Plan include a clear reporting and evaluation mechanism, so that progress on technology-related initiatives can be tracked and reported publicly over the life of the plan.

We encourage the Government to ensure strong alignment between the Second Action Plan and the concurrent Second Action Plan under the National Strategy to Prevent and Respond to Child Sexual Abuse 2021–2030, given the significant overlap in technology-facilitated harms, system responses, and the populations served.

ICMEC Australia would welcome the opportunity to provide further information or to meet with the Department to discuss our submission.

Submission contact:

 – Head of Government Affairs and Law Enforcement Outreach

