December 2023

eSafety Commissioner's Industry Standards Public Submission

International Centre for Missing and Exploited Children (ICMEC) Australia

ICMEC Australia would like to express our strong support for the eSafety Commissioner's efforts to prioritise the online safety of children in the latest draft industry standards.

The codes, focusing on *Relevant Electronic Services* and *Designated Internet Services,* look to amend two key online platforms that threaten children's safety, and may allow child sex offenders to manipulate technology to abuse and exploit children.

ICMEC Australia supports a whole-of-ecosystem approach to child protection with an emphasis on proactively removing child sexual exploitation material from the internet. We strongly believe that a cross-industry, collaborative approach is critical to combat this heinous crime.

Research states that this is a problem that doesn't just happen across international borders - it's also very much an Australian problem. The work that the eSafety Commissioner is doing to strengthen our nation's response to this crime is critical.

In the 2022-23 financial year, the Australian Centre to Counter Child Exploitation received 40,232 reports of child sexual exploitation. Each image and video is known to be a crime scene, and real children are the victims.

ICMEC Australia welcomes the strength of the updated codes in their emphasis on the **disruption** and **deterrence** of child sexual exploitation. The latest codes are strong in their requirements for the relevant platforms to prevent child sexual abuse material from being shared or distributed through technology.

ICMEC Australia echoes the call for a preventative approach to eliminating this crime. We support the call for platforms (with more than one million active monthly users) in Australia to:

a) have a program of investment in this technological space; and

b) have a strong focus on the further development of tools to disrupt and deter CSAM on their platforms.

Amidst the rapid technological changes and the growth of new and emerging technologies (such as generative Artificial Intelligence - AI), technology poses an added challenge to the regulation of child sexual exploitation online. The eSafety Commissioner has already flagged an increase in AI-generated child sexual abuse material this year, and we know the numbers will continue to grow.

The strengthening of Industry Codes for child protection and the acknowledgement that "*generative AI functionality could be misused to generate class 1A or class 1B material*"[1] is an important addition by the Office of the eSafety Commissioner which we firmly support.

[1] Discussion Paper, page 21

ICMEC Australia applauds the Commissioner's prioritisation of the safety of children in applying the codes to an extensive range of online services including:

- Application of the 'Designated Internet Service Standard,' for providers who offer generative AI features, machine learning model platform services, and enterprise designated internet services that also provide upstream generative AI services; and
- Acknowledging the risks posed by open-source generative AI model services by all providers in this industry.

We are privileged to have a number of subject matter experts as part of our team at ICMEC Australia and our team may be able to provide specific technical feedback on some of the new draft codes, should the Commissioner be interested. In particular we believe we could assist in further conversations around questions 4, 5, 6, 10, 16 and 23, listed within the Discussion Paper (Appendix A), and we would be open to roundtable discussions or one-on-one conversations if suitable.

Our work at ICMEC Australia is underpinned by the deep understanding that the crime of child sexual exploitation and abuse affects far too many children both in Australia and beyond our borders. The latest draft online safety standards are another step in the right direction to establishing strong regulatory standards that will lead to safer outcomes for children everywhere.

ICMEC Australia offers strong endorsement and support for the industry codes, and resolutely echoes the Australian eSafety Commissioner's commitment to stronger protections for all children.

Anna Bowden

Chief Executive Officer
ICMEC Australia
[redacted]

Appendix A

Areas where ICMEC may be able to assist in advice at roundtable meetings/or to provide advice as required.

4. Is the technical feasibility exception in the obligation to detect and remove known child sexual abuse material and pro-terror material appropriate? How effective will this obligation be with this exception?

We have concerns that technical feasibility as an exception is problematic. It may leave platforms with limited responsibility to prioritise the safety of children above all else. We would suggest stronger wording or more rigor in the exceptions.

5. Are there other examples of systems, processes, and technologies that can detect, flag and/or remove known child sexual abuse material and known pro-terror material at scale, which should be highlighted in the Standards or accompanying guidance?

The integration of hash matching technologies, machine learning and artificial intelligence tools to scan for known material is a key example of how to prioritise the safety of children by using relevant technologies. This is something we could assist with in a roundtable conversation with some of our subject matter experts.

6. Are there any limitations which would prevent certain service providers from deployment systems, processes and technologies to disrupt and deter child sexual abuse material and pro-terror material on relevant electronic services? If there are limitations, how might these be overcome? Is it appropriate for this requirement to apply to gaming services with communication functionality?

Our law enforcement stakeholders have stated to us that there has been an increase in child sexual abuse and exploitation through gaming services as of late, so the need for a strong response on these platforms is echoed by ICMEC Australia.

10. Should the requirement on certain relevant electronic services to respond to reports of class 1A and class 1B material on their service be limited to a requirement to take 'appropriate action'?

The phrase 'appropriate action' leaves room for discretion on the part of service providers, when the emphasis should be on what is in the best interest of children. We would support stronger wording in this space to strengthen the intent.

16. Do the draft definitions for high impact generative AI designated internet service and machine learning model platform service capture the right services? Are there types of providers that should not be included or should be excluded?

From current understanding, the Commissioner's definitions of GenAI and machine learning services capture an all-encompassing variety of service providers.

However, it must be noted that the rapid rate by which this technology advances poses questions that the codes might not be able to encompass all future technologies, and the definitions may need to be updated on a semi-regular basis.

23. Is the technical feasibility exception in the obligation to detect and remove known child sexual abuse material and pro-terror material appropriate? How effective will this obligation be with this exception?

*This is difficult to comment on without the technological understanding but our team do have expertise in some of these matters and would be willing to assist in further discussions around this issue.