5 August 2025

To: The Office of the Australian Information Commissioner (OAIC)

RE: Consultation on Children's Privacy Code

The Institute of Electrical and Electronics Engineers (IEEE) Standards Association (IEEE SA) welcomes the opportunity to provide its comments regarding the development of a child's privacy code in Australia.

IEEE SA is a globally recognized standards-setting body within IEEE, the largest organization of technology professionals in the world dedicated to advancing technology for the benefit of humanity. IEEE SA provides a globally open, consensus-building environment that enables people and entities to work together to develop market-relevant technology standards, while developing approaches and solutions to help shape a better, safer and sustainable world.

IEEE SA would like to suggest that the development and use of technical standards and goal to foster a safer online environment and posits that age-appropriate design, grounded in ethical, privacy-respecting and standards-based technological frameworks is essential for helping to safeguard not only children but all vulnerable age groups online.

Global standards are a critical enabler for adoption of practical implementation mechanisms that are based on a structured approach for age verification that preserve privacy and respect the rights of the child.

Such global standards are valuable resources for the technical community as they provide principled frameworks that help bridge the gap between privacy and policy objectives, and practical implementation.

The value of adhering to a standards-based approach in developing and deploying product development and compliance to standards can help mitigate potential risks as well as to enable interoperability between products and within systems to ensure children are uniformly protected.

IEEE Responses to Specific Questions from the Request for Feedback

1. Scope of services covered by the Code

Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view. (An 'APP entity' is defined to be an agency or organization)

Yes, there should be a separate class of entity for AI, and in particular, AI partnerships (also called companions, empathetic partners. Personal AI, co-pilots, assistants, and related phrasing

for human-AI partnering. These types of APP entities have particular characteristics and behaviors that mimic human behavior, and can introduce particular risks for use by children, as they can be confused with 'real' relationships

For example, **IEEE 7014-2024TM Standard for Ethical Considerations in Emulated Empathy in Autonomous and Intelligent Systems**, and the forthcoming **IEEE P7014.1TM Recommended Practice for Ethical Considerations of Emulated Empathy in Partner-based General-Purpose Artificial Intelligence Systems** are standards that provide guidance and actions for the ethical development, deployment, or decommission of autonomous and intelligent systems that attempt to emulate aspects of human empathy. They cover issues of emulated empathy in AI systems that use 'emulated empathy' in general purpose AI systems for human-AI partnerships, including products marketed as empathetic partners, personal AI, co-pilots, assistance, AI companions and other terms for human-AI partnering.

Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

The Code should include criteria in the scope of the Code to define and clarify what is "real", what is "simulated" as a child might be reasonably confused as to what is 'real' or 'simulated' in a relationship with an AI generated entity. In particular to address where a child might be reasonably confused or misled or have their developing critical analysis facilities confused or compromised. This pertains in particular to Generative AI applications.

2. When and how the Code should apply to APP entities

'Likely to be accessed by children' is the same standard as the UK's Age Assurance Design Code. Is there any evidence as to the practical effectiveness of the threshold in that context?

Not in the case of access to human-AI partnering. These services are likely to be accessed by children and adults alike.

What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?

It would be wise to assure that the APP entities likely to be accessed by children, unless there may be some sort of physical barrier to access (i.e. within an adults-only location), follow a standard such as **IEEE 2089-2021™ Standard for an Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children**. There are no reliable boundaries on the World Wide Web (WWW), and hence it is likely that children will and can be exposed to all content unless a clear framework is adopted.

What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?

One approach is to consider establishing a framework for the design, specification, evaluation, and deployment of online age verification systems such as the framework found in **IEEE 2089.1™-2024 IEEE Standard for Online Age Verification.**

Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

IEEE has several standards that address emulated empathy in AI systems, in particular 'emulated empathy' in general purpose AI systems for human-AI partnerships, including products marketed as empathetic partners, personal AI, co-pilots, assistance, AI companions and other terms for human-AI partnering. For example, **IEEE 7014-2024(™) Standard for Ethical Considerations in Emulated Empathy in Autonomous and Intelligent Systems**, and the forthcoming **IEEE P7014.1(™) Recommended Practice for Ethical Considerations of Emulated Empathy in Partner-based General-Purpose Artificial Intelligence Systems** are standards that discuss the issue of emulated empathy in AI systems.

Also the IEEE standard **IEEE 2089-2021™ Standard for an Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children** offers a range of alternative approaches that APP entities could take to meet their obligations under the Code, including taking a child-centric view of data use to:

- Minimize or eliminate behavioral nudging and coercion, by turning off persuasive features that push engagement by default, turning off features that lessen privacy by default, and ensuring that automated processes optimized for commercial purposes do not infringe on children's rights or undermine their needs.
- Minimizing or eliminating the commoditization of data by only collecting and retaining the minimum amount of personal data a product or service needs, providing age appropriate information that helps explain what data or activities are being shared, a and by not disclosing, selling, or sharing children's data unless there is a demonstrable and non-commercial reason to do so, with the best interests of the child over commercial interests, and not profiling children for targeted advertising

Are there classes of APP entities, personal information, or activities of entities, for which different requirements under the Code may be appropriate? If so, what considerations should inform that approach?

In the case of access to and use of human-AI partnering, that should be a separate class of APP due to the high risk of privacy violation and additional risks for children. In the case of access to Generative AI applications, it should be a separate class of APP due to the high risk of privacy violation and additional risks for children.

How should the Code accommodate for the varying roles, functions and risk profiles of different kinds of services, activities or personal information?

IEEE 2089-2021™ assumes that all "users" of services also includes those whose personal data is held in a system, whether they have access to that data or are aware of that data or not. For children, there cannot be a presumption that they are able to assess the risk or benefits of use of any system or application nor informing them of their rights or trying to meet their needs. Nor

can it be assumed that all children have a parent or adult present who is engaged, literate, skilled or able to act on their behalf.

The Code must consider that all accessible services and products (meaning all services and products) consider the vulnerabilities associated with children according to their age and are age appropriate by default.

3. Age range-specific guidance

Would age-based guidance be appropriate and assist APP entities in tailoring protections and interfaces appropriately and effectively?

Yes, it would be appropriate. **IEEE 2089-2021™** offers much guidance in this area, including the following guidance to APP entities for tailoring protections and interfaces.

Offer a service appropriate to the age of the user, which includes the following:
1) Reduce and address harmful content.
2) Reduce and address harmful contact.
3) Reduce and address harmful conduct as follows: i) ii) Uphold community rules. Offer a high bar of moderation. iii) Offer swift and easy access to expert advice. iv) Offer swift and easy access to redress
4) Reduce and address harmful contract risks.
5) Offer a high bar of data protection.
6) Reduce automated recommendation of harmful material.
7) Prevent products and services from recommending poor quality information.
8) Protect from design features that extend use, particularly at night.
9) Encourage time off.

Section APP specific questions

4. APP 1 – open and transparent management of personal information

What communication methods should APP entities use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds?

IEEE 2089-2021™ offers the following advice:
Require and obtain valid, informed, and meaningful consent that is transparent about the risks associated with the nature and features of product or service. Valid and meaningful consent shall be obtained from children and, where necessary, parents or a responsible adult, consistent with all applicable laws and regulations. Verification of inclusivity, by a variety of means including by offering content in local languages, including moderation and redress, considering the needs of vulnerable groups and protect specific group's gender, race, ethnicity, or sexuality, considering the needs of children who may not have active parents or caretakers, considering the affordability of the product or service, by verifying accessibility for children and the variety of their different needs of children with different needs.

How should APP entities ensure APP1 obligations are met when their services are used by both adults and children, particularly when children are not the intended primary users?

Ensure that children's needs are addressed as a minimum baseline for the product or service.

What should be considered under the 'reasonable steps' test when implementing internal practices, procedures and systems for managing children's personal information?

IEEE 2089-2021™ guides what the 'reasonable steps' should be for moderation and redress.

6. APP 3 - collection of solicited personal information

What does 'lawful 'and 'fair' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?

IEEE 2089-2021™ specifies the meaning of 'fair terms' as follows: those terms that meet the reasonable expectations of children (and parents) and that verify that fair published terms are met and legal obligations to children are upheld.

IEEE SA welcomes the recognition that children must be able to discern when they are interacting with an AI system.

AI must not be considered solely within the scope of "user support measures" such as chatbots.

AI systems are increasingly integrated into the core functionality of online platforms accessed by children — including recommender systems, content generation, automated moderation, and adaptive interfaces. These systems can significantly influence children's behavior and well-being.

The guidelines should therefore include additional provisions addressing:

- Clear and age-appropriate signaling when a child interacts with an AI system.
- Documentation and transparency requirements for AI systems that materially affect minors.
- Auditable safeguards to mitigate harms from generative models or automated decision-making.

IEEE SA would also like to note that its communities have developed a collection of standards globally recognized in age-appropriate design, applied ethics and systems engineering and continues to develop accessible and sustainable approaches and solutions for pragmatic application of AI systems principles and frameworks in partnership with leading child rights organizations, such as the 5Rights Foundation.

Here is a listing of adopted standards, both approved and ones still in development (the former indicated with the approval year, the latter with a "P" preceding the numeric designation), for consideration:

IEEE 2089-2021™ Standard for an Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children sets out processes through the life cycle of development, delivery and distribution, that will help organizations ask the right relevant questions of their services, identify risks and opportunities by which to make their services age appropriate and take steps to mitigate risk and embed beneficial systems that support increased age appropriate engagement.

To note, this standard serves as the basis for the CEN/CENELEC Workshop Agreement CWA 18016 for Age appropriate digital services framework, based on IEEE 2089.

IEEE 2089.1™-2024 IEEE Standard for Online Age Verification establishes a framework for the design, specification, evaluation, and deployment of online age verification systems
.

IEEE P2089.2™ Standard for Terms and Conditions for Children's Online Engagement defines processes and practices to develop terms and conditions that help protect the rights of children in digital spheres. The standard helps avoid nudging, manipulation, and data exploitation that violate the interests of children. Furthermore, the standard enables providing data agency and ownership to children.

IEEE P2089.3™ Standard for Online Parental Consent establishes a framework for the design, specification, evaluation, and deployment of online parental consent systems.

IEEE P2863™ Recommended Practice for Organizational Governance of Artificial Intelligence specifies governance criteria such as safety, transparency, accountability, responsibility and minimizing bias, and process steps for effective implementation, performance auditing, training and compliance in the development or use of artificial intelligence within organizations.

IEEE P3462™ Recommended Practice for Using Safety by Design in Generative Models to Prioritize Child Safety follows a safety by design approach by providing recommendations for developing, deploying, and maintaining generative artificial intelligence models with adequate safeguards against child sexual abuse. The document provides a framework that expands child safety to the entire lifecycle of machine learning (ML): development, deployment, and maintenance stages. Each part in the process includes opportunities to prioritize child safety, regardless of data modality (i.e. text, image, video, audio) or whether an organization releases its technology as closed source or open source, or some release option between these two.

IEEE 7000™ Standard Model Process for Addressing Ethical Concerns during System Design incorporates a set of processes by which organizations can include consideration of ethical values throughout the stages of concept exploration and development Processes incorporated in the standard provide for traceability of ethical values in the concept of operations, ethical requirements, and ethical risk-based design are described in the standard.

IEEE 7001-2021™ Standard for Transparency of Autonomous Systems establishes measurable, testable levels of transparency, so that autonomous systems can be objectively assessed, and levels of compliance determined.

IEEE 7002™-2022 Standard for Data Privacy Process contains requirements for a systems/software engineering process for privacy-oriented considerations regarding products,

services, and systems utilizing employee, customer, or other external user's personal data.

IEEE P7008™ Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems establishes a delineation of typical nudges (currently in use or that could be created). It contains concepts, functions and benefits necessary to establish and ensure ethically driven methodologies for the design of the robotic, intelligent and autonomous systems that incorporate them.

IEEE P7012™ Standard for Machine Readable Personal Privacy Terms identifies/addresses the manner in which personal privacy terms are proffered and how they can be read and agreed to by machines.

For more IEEE AI-related standards please see:
https://standards.ieee.org/initiatives/autonomous-intelligence-systems/

Certification

IEEE has a certification program, called IEEE **CertifAIEd™**, which offers a risk-based framework supported by a suite of AI ethical criteria that can be contextualized to fit organizations' needs – helping them to deliver a more trustworthy experience for their users. IEEE CertifAIEd Ontological Specifications for Ethical Privacy, Algorithmic Bias, Transparency, and Accountability are an introduction to our AI Ethics criteria.

It also has the IEEE Online Age Verification Certification Program, which assesses the design, specification, evaluation, and deployment of age verification systems against the framework identified in the IEEE 2089.1™, Standard for Online Age Verification. It helps Digital Services Providers, Policymakers, and Regulators to Address Requirements From Various Jurisdictions Around the World, including:

- Appropriate Design Codes in the UK, California and more
- Europe's Digital Services Act, General Data Protection Regulation (GDPR), and Audiovisual Media Services Directive (AVMSD)
- US's Children's Online Privacy Protection Act (COPPA)
- India's Digital Personal Data Protection Act (DPDPA)

Age Verification Can Help Organizations to:

- Recognize that the user may be a child.
- Present content and terms in an age-appropriate manner.
- Offer a level of validation for service design decisions by deploying processes and best practices.
- Help ensure their marketing efforts target age-appropriate audiences and align with applicable regulations protecting minors.
- Build consumer trust and maintain a reputation as a responsible brand.
- Mitigate risk associated with the creation of fraudulent online accounts.

IEEE SA AI-Related Programs and Initiatives

The IEEE SA has a portfolio of programs and initiatives in the pre-standardization space, where individuals and groups explore various topics and outline standards roadmaps and other outputs to help inform the standardization ecosystem. In the AI space, programs include:

The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems

Bringing together experts in fields related to autonomous systems (e.g., Robotics, Artificial Intelligence, Computational Intelligence, Machine Learning, Deep Learning, Cognitive Computing, Affective Computing) to identify and address the ethical considerations related to the design of autonomous systems and the issues they involved.

Ethical Principles for Engineering Digital Services for Children

Introducing concrete ethical principles that may easily be adhered to and endorsed by industry participants enables IEEE to be an important resource providing vital tools and support to industry participants in developing their technologies in a manner that benefits humanity.

Synthetic Data

Synthetic data is artificial data that is generated based on original customer data. It is highly realistic and statistically representative to the original data and thus suitable to serve as a drop-in replacement for it (e.g., for AI training). Yet – when generated with appropriate privacy mechanisms – synthetic data is fully anonymous and impossible to re-identify.

IEEE SA commends the OAIC proactive approach to implementing the Children's Online Privacy Code and supports the development of robust, enforceable and technically grounded guidelines to protect minors online.

IEEE SA stands ready to collaborate with Australian institutions, regulators and industry stakeholders to promote safe, ethical and age-appropriate digital ecosystems and would welcome the opportunity to contribute its technical expertise to regulatory codes of conduct, or further refinement of enforcement guidance under the Children's Online Privacy Code.

If you have questions, please do not hesitate to contact [redacted]