

Response to the *Official Exposure Draft of the Children's Online Privacy Code*.

Written by [REDACTED]
[REDACTED]

We provide the following feedback on the *Official Exposure Draft of the Children's Online Privacy Code* (hereafter referred to as the Code):

1. We note that the Code includes educational apps, games and websites and online school management systems that monitor student performance. It is unclear whether the Code applies to educational apps, games and websites that are currently or will be used in Australian schools and early childhood centres. There is weak regulation of educational technology for student privacy in Australian schools [1]. Local and international research indicates that educational apps, games and websites used by schools and learning management and school administration systems are collecting, sharing and selling children's information often across borders at scale [2, 3]. The Code should make it clear that Australian schools, early childhood centres and schooling system administrators such as state departments of education must comply with the Code.
2. Reference to "online school management systems that monitor student performance" should also specify learning management systems (LMS) as these are considered different to administrative management systems in schools. There is limited clarity in Australian schools regarding what type of student data LMS collect, use, share and sell. Schools mandate LMS use with students effectively unable to contest or refuse to use the platform as it is the foundation to online learning and communication. Compulsory educational technology adoption in schools whether it be an LMS or educational app/system is highly problematic to the notion of voluntary, informed consent [4].
3. Related to the above point, research indicates that general digital applications and platforms recommended to students for homework purposes are tracking student activity from in-school systems to out-of-school systems [5]. This supports the need to include Australian schools and early childhood centres in the Code.
4. Regarding section 28. 2 (g) on automated decision-making including profiling, educational apps and platforms used in schools increasingly use predictive and prescriptive learning analytics that effectively profile students [1]. Educational applications such as intelligent tutoring systems have adaptive curriculum and assessment and pedagogical agents that rely on profiling student learning and automated exposure to content and learning pathways. LMS also include such analytics with recommender and predictive components and visualised profiles of students. It should be clear that these school based technologies fall under section 28. 2 (g).
5. The Code does not expressly address the use of artificial intelligence, especially when discussing automated decision-making. This omission is particularly significant as schools increasingly deploy plagiarism and AI-writing detectors to assess learning and flag academic-integrity cases. These systems often process sensitive biometric and behavioural data, and their models are opaque and difficult to contest due to the lack of transparency. The documented false-positive and demographic-bias rates in terms of academic misconduct cases [] mean children may be wrongly classified as dishonest with limited recourse. The opaque retention protocols of such scores will also mean that the integrity flags persist and follow children beyond their immediate purpose. The code should expressly name AI/ML integrity- and assessment tools within "automated decision-making".

6. We note that there is reference to geolocation data in the *Official Exposure Draft of the Children's Online Privacy Code* and its associated child and parent friendly resources. One of the most pressing emerging threats to privacy is the large scale automated harvesting of biometric and contextual data which is considered sensitive data under the *Privacy Act 1988* (Cth). Biometric data is highly identifying and increasingly used for identification and verification purposes. Educational technologies and those used by children often collect biometric, affective and contextual data through sensor technology and this should be explicitly addressed in the Code and children and parent resources.

7. Digital fraud in the forms of scams and cyber extortion are increasingly prevalent for under 18's in Australia. In 2025, young people reported losses of \$35,502 to: buying and selling scams, identity take over scams and phishing. The top contact methods were: online, text message and email [7]. It is believed that most of the scams aren't reported for this demographic and anecdotal evidence is showing that 1 in 5 under 18's are affected by scams. Despite the social media ban in Australia, via the *Online Safety Amendment (Social Media Minimum Age) Act 2024*, scammers can still contact and blackmail young people to extort money. Sextortion [8] of teens for example has been taking place in Australia for some time [9].

8. There is no mention of financial data in the draft Code but the Code does refer to the *Privacy Act 1988*, where financial data such as, bank account details, income, transactions is "personal information". Many young people have part-time jobs and we think that financial data should be specified in the Code. Likewise, there is no mention of health data but the Code does refer to the *Privacy Act 1988* where health data such as, physical, mental, psychological health, genetic data and information collected while providing a health service is classified as "sensitive information". Again, we think that there should be specific reference to children's health information.

9. There is no mention of "data breach" or "data leak" in the draft Code, again a specific reference to these terms is required and additionally, a breach or leak of children's data should result in a higher duty of care.

10. There are many mentions of "age appropriate", in the draft Code, this term is difficult to define and guidance is required in the Code and supporting documentation.

11. There are many mentions of "consent" in two categories i) children who are under 15 years of age and ii) children who are at least 15 years of age. This puts the onus on providers of online content to ascertain but children's ages are difficult to monitor, and further guidance is required when referring to these categories.

12. Division 7—Making inquiries and complaints is a very helpful addition. Perhaps there needs to be more detail for children to actually make a complaint themselves if they need to. This would encourage "children's voices" and provide an opportunity to take their concerns seriously.

13. Penalties for contraventions of the Code are not clear and while we understand that the Code operates as an extension of the *Privacy Act 1998* (Cth), the pressing issues at stake urge us to request and recommend that penalties in the *Privacy Act 1998* (Cth) be referred to within the Code as well as references to contact points such as, the OAIC and the information commissioner so that young people can be assured that contraventions of the Code will be taken seriously.

References

1. Southgate, E., Naghizade, E., Corman, A., & Atherton, M. (2025). Towards a governance roadmap for educational technology in Australian schools. *The Australian Educational Researcher*, 52(6), 4703-4730. <https://doi.org/10.1007/s13384-025-00916-3>
2. See research from UNSW https://www.unsw.edu.au/newsroom/news/2026/04/australian-children-data-at-risk-through-approved-school-apps?utm_id=97758_v0_s00_e232_tv2_tp1_a1demo0jqcz7qi
3. Internet Safety Labs. (2022). 2022 K-12 EdTech safety benchmark: National findings – Part 1. Internet Safety Labs. <https://internetsafetylabs.org/wp-content/uploads/2022/12/2022-k12-edtech-safety-benchmark-national-findings-part-1.pdf>
4. Walker, K. L., Bodendorf, K., Kiesler, T., de Mattos, G., Rostom, M., & Elkordy, A. (2023). Compulsory technology adoption and adaptation in education: A looming student privacy problem. *Journal of Consumer Affairs*, 57(1), 445-478. <https://doi.org/10.1111/joca.12506>
5. Day, E., Pothong, K., Atabey, A., & Livingstone, S. (2024). Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. *Learning, Media and Technology*, 49(3), 356-370. <https://doi.org/10.1080/17439884.2022.2152838>
6. Hadra, M., Cambridge, K. & Mesbah, M. (2026) Evaluating the accuracy and reliability of AI content detectors in academic contexts. *International Journal for Educational Integrity*, 22 (4). <https://doi.org/10.1007/s40979-026-00213-1>
7. Australian Government, Scamwatch, *Scam statistics – scam types 2020 to 2025*, [Scam statistics – scam types 2020 to 2025 | Scamwatch.](#)
8. Ricon, Tsameret. (2026). Beyond rules: A focused comparative vignette analysis of how public AI systems interpret sexual coercion, privacy abuse, and grooming in adolescent digital scenarios. *Computers in Human Behavior: Artificial Humans* (2026), 100320.
9. Foster, A. January 16, 2023, "Australian teenagers targeted by sick sextortion scams" <https://www.news.com.au/technology/online/security/australian-teenagers-targeted-by-sick-sextortion-scams/news-story/ae6975b8308917f611b03fa99bd2b0d9>