CHILD WISE
creating child safe communities

Executive Manager, Investigations
Office of the eSafety Commissioner
submissions@esafety.gov.au

Dear Executive Manager,

RE: Submission to the Restricted Access System Declaration Online Safety Act 2021 Discussion Paper

Thank you for the opportunity to respond to the *Restricted Access System Declaration Online Safety Act 2021 Discussion Paper* (the Discussion Paper). While the Discussion Paper is definitely a step forward in the policy and legislative landscape protecting children, Child Wise fears that the current direction of the *Online Safety Act 2021* misses the paramount and vital opportunities to:

- **Address the complexity of tackling content in social media, particularly user-generated or user-posted content, and could potentially have the opposite to the intended effect. Such complexity must be well understood in the development of any Restricted Access System (RAS), to ensure that safety is carefully balanced with children's rights to access information and express themselves;**

- **Ensure children can continue to be legitimate users of social media, while the risks are minimised. While Child Wise supports the implementation of Restricted Access Systems in specific circumstances across relevant websites, online advertising, social media and gaming, it does not support one-size-fits-all solutions to this complex problem, particularly in social media services that are designed for, and used by, children as a key part of their everyday lives. It is imperative that in protecting children from such harm, the regulation does not inhibit access to services that many young people would consider essential, and which may contribute to safety and wellbeing, e.g. access to support services, information and pro-social connection.**

- **Protect children who aren't end-users, but generate or post content, without understanding the seriousness of the content or the offence. In this context, Child Wise supports an increasing focus on education for children, parents and guardians.**

- **Recognise the full gamut of harms that require protection. Only a narrow set of contexts for harm are protected under the proposed legislation.**

- **Regulate and implement the RAS in the context of gambling and gaming, given their potential damage to a child's healthy development.**

This Child Wise submission responds to several questions outlined in the Discussion Paper.

Discussion Paper Question 1: Under the Online Safety Act 2021, the RAS will only apply to Restricted Material that is provided from Australia on a social media service, relevant electronic service or designated internet service, or that is hosted in Australia. What elements should be part of an effective system to limit access to that kind of material?

Child Wise Response:

- Child Wise supports the report of the House of Representatives Standing Committee on Social Policy and Legal Affairs following its inquiry into age verification for online wagering and online pornography, *Protecting the age of innocence* (February 2020), and its key principle that we should protect children online, just the way we do in the physical world:

  "*In face-to-face commerce, children and young people are restricted from accessing a range of adult products and services at the point of sale. This includes alcohol, tobacco, and mobile phone services. Here, potential consumers are required to show appropriate personal identification before accessing these products.*

  The Committee considers that the same principle should apply to access online pornography and online wagering… outside the scope of this inquiry, it was also put to the Committee that online sales of alcohol should similarly be restricted to individuals whose age has been verified using an effective method. As a matter of principle, the Committee accepts this proposition."

- Child Wise supports the focus on R18+ or Category 1 Restricted ('Restricted Material') under the National Classification Code as well as X18+ material. Child Wise notes that R18+ or Category 1 Restricted material includes realistically simulated sexual activity between adults, high impact nudity, high impact violence, high impact drug use and high impact language.

- Child Wise supports the intent of the *Basic online safety expectations* as outlined in the *Online Safety Act 2021 (Cth)* Part IV div 2, which outlines the overarching expectations that providers of online services will take reasonable steps to ensure that end-users are able to use the service in a safe manner and importantly, that they will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to inappropriate material.

- Child Wise notes the *Online Safety Act2021 (Cth)* focus on cyber bulling, cyber-abuse, non-consensual images and material that is considered to promote, incite, instruct or depict abhorrent violent conduct as defined in Subdivision H of Division 474 of the *Criminal Code*.

- Child Wise notes that the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth)* defines abhorrent violent conduct as terrorist acts, murder of another person, attempted murder of another person, torture of another person, rape of another person or kidnapping of another person.

The legislation still needs to address the complexity of tackling content on social media, particularly user-generated or user-posted content.

- Child Wise notes that not all harmful content to children will meet the criteria noted in the *Online Safety Act 2021 (Cth).* While at times the restriction of access to minors is very clear (for example, as is the case with commercial online pornography or abhorrent violent conduct as defined above), the proliferation of user-generated or user-posted content shared via social media platforms that are themselves not focused on the production and/or distribution of such material, is a very complex policy and regulatory issue.

- Children can develop content that is either intentionally or unintentionally harmful to other viewers. The dimension of such content requires monitoring and regulation. Additionally, vulnerable adults can be caught by predatory behaviour that seeks to elicit self-made material and then be used as blackmail. This activity may be below the Act's threshold, but remains a concern that should afford protection.

- Child Wise is concerned that such complexity must be well understood in the development of any Restricted Access System, to ensure that safety is carefully balanced with children's rights to access information and express themselves.

- Further, the complexity of social media platforms, and the ways in which they distribute and target content to children, must be understood and contextualised.

- For example, Child Wise notes recent bodies of academic evidence that document increasing access to content by children via social media that promotes non-suicidal self-injury (NSSI) and eating disorders (see for example *Logrieco, G., Marchili, M. R., Roversi, M., & Villani, A., 2021*). The same research notes:

  "The application algorithm records data from the single users and proposes videos that catch the kid's attention specifically, by creating a personalized "For You" page.

  This feed will suggest videos from anyone on the platform, not just from the followed accounts.

  Therefore, if a user accidentally views a video dealing with anorexia on the homepage and, intrigued, searches for other videos alike, the algorithm will keep suggesting such videos, contributing to the development of obsessive behaviours…..

  These algorithms, with the aim of increasing the diffusion of user sensitive virtual content, are based on solid models whose development is still ongoing.

  However, these algorithms are not yet able to discriminate harmless and harmful content, as this, rather than the videos they like, is related to the user's own life experience, which cannot be embedded in the formula".

Ensuring children can continue to be legitimate users of social media

- While Child Wise supports the implementation of Restricted Access Systems in specific circumstances across relevant websites, online advertising, social media and gaming, it does not

support one-size-fits-all solutions to this complex problem, particularly in social media services that are designed for, and used by, children as a key part of their everyday lives. It is imperative that in protecting children from such harm, the regulation does not inhibit access to services that many young people would consider essential, and which may contribute to safety and wellbeing, e.g. access to support services, information and pro-social connection.

- Of relevance to the current COVID-19 lockdowns, Child Wise notes research that emphasises how important access to social media services/forums has been for children and adolescents. For example, research published in the Italian Journal of Paediatrics (*Salzano, G., Passanisi, S., Pira, F., Sorrenti, L., La Monica, G., Pajno, G. B., Pecoraro, M., & Lombardo, F., 2021*) notes:

  "Technology, and particularly social media, were fundamental to allow youth to overcome this stressful period and to limit psychological adverse events related to the lock-down.

  The use of technology was predominant both for recreational activities (communications, games, videos) and for educational purposes (scholar, musical, and sportive activities)…. Almost all the subjects declared having a social profile (i.e. Instagram, Facebook, Tik Tok, Twitter, Snapchat, Ask.fm). Smartphones were mainly used to message, chat, or video-chat with other people, and to browse the web.

  Technology has played a crucial role during the quarantine for young subjects who have increased the daily use of technological devices to stay connected with the rest of the world. Particularly, social media platforms have become fundamental for maintaining and enhancing socialization. These interactive media platforms have been constantly used to maintain friendship and emotional connection. Nowadays, the real-life of adolescents is closely related to their "online environments", and social media have become an integral part of critical adolescent developmental task

  Social media tools also allow adolescents to enhance individual and collective creativity through the sharing of artistic and musical activities, the creation of blogs, podcasts, and videos

  The use of social media tools can also facilitate self-esteem increase, identity exploration, aspirational development, and it provides adolescents the opportunity to explore knowledge and establish new friendships."

Remembering that end-users can be children

- Child Wise supports the requirements within the *Online Safety Act 2021 (Cth)* that hosting provisions, social media services or others take all reasonable steps to ensure the removal of identified content by the Commissioner, within 24 hours. Child Wise notes that penalties for non-compliance may include 500 penalty units (1 penalty unit is currently equivalent to $110).

- Child Wise notes and supports powers that equally require end-users to remove content identified by the Commissioner.

- However, Child Wise notes that children are also end-users who generate or post content, and may not understand the seriousness of the content or offence. In this context, Child Wise supports an increasing focus on education for children, parents and guardians.

Discussion Paper Question 5: What factors should be considered when assessing the effectiveness and impacts of systems, methods and approaches to limiting access or exposure to age-inappropriate material?

Child Wise Response:

- Child Wise notes and supports the overarching objectives of the *Online Safety Act 2021 (Cth)* pt IX div 1 which states that the objective of Restricted Access Systems is *protecting children from exposure to material that is unsuitable for children*.

- Child Wise notes the Australian Government's interest in age-verification systems as a key component of a RAS.

- Child Wise reiterates that such systems can be effective and appropriate in very clear circumstances (such as commercial online pornography), however it may be far more difficult to implement in social media settings designed for children who are mostly over the age of 13 years.

- Age verification systems must be robust, effective, highly tested and able to evolve at the pace that technology evolves. Child Wise works with sector partners in the UK whose research demonstrates high levels of accuracy. This could mitigate against the risk of inadvertent 'net widening', but the key point is that the Act's operationalisation must rely on the introduction of age verification technology which can consistently demonstrate accuracy with a limited margin of error.

Discussion Paper Question 6: What systems, methods and approaches do you consider effective, reasonable and proportionate for verifying the age of users prior to limiting access age-inappropriate material?

Child Wise Response:

- Child Wise notes research by Pasquale, L., Zippo, P., Curley, C., O'Neill, B., & Mongiello, M. (2020) that suggests the following strategies to support limiting access or exposure to age-inappropriate material:

> *Apps should apply the most restrictive privacy settings by default for any user that declares themselves to be under the age of 18. For example, photos, posts and messages*

should only be shared with "friends", location data should not be collected at all. It should also not be possible to override privacy settings without explicit parental consent.

Encourage users not to lie about their age. Despite the presence of a minimum age requirement, many underage users continue to use social and communication apps. Thus, users must be incentivised to be honest about their age, with minimal data being collected in this case. Giving a user an option to go back and change their date of birth in order to bypass any restrictions encourages them to lie about their age. Providing mechanisms that deter a user from installing an app on a device on which they have previously declared themselves to be underage is currently the most sensible solution and the hardest to circumvent.

Implement Robust Age Verification Mechanisms. Where a minimum age requirement is put in place, it should be backed up by appropriate age verification mechanisms. We recommend age verification as an ongoing process that does not terminate after sign-up. For example, age verification can analyse information generated from the use of an app (e.g., texts, content exchanged).

- Child Wise supports the emerging development and application of Artificial Intelligence being used to implement ongoing age verification processes that are continuous, well beyond sign-up. These seem to be effective ways to ensure user safety without limiting a user ability to join such services. For example, Child Wise notes the following comment from Facebook (https://about.fb.com/news/2021/07/age-verification/):

  "Many argue that collecting ID is the answer to this industry problem, but there are significant limitations to this approach: many young people don't have an ID, ID collection isn't a fair or equitable solution, nor is it foolproof. Access to government IDs varies depending on where you live in the world…

  Artificial intelligence is the cornerstone of the approach we're taking. We've developed technology that allows us to estimate people's ages, like if someone is below or above 18.

  We train the technology using multiple signals. We look at things like people wishing you a happy birthday and the age written in those messages, for example, "Happy 21st Bday!"…

  We also look at the age you shared with us on Facebook and apply it to our other apps where you have linked your accounts and vice versa — so if you share your birthday with us on Facebook, we'll use the same for your linked account on Instagram."

- Child Wise is aware of extensive political and academic commentary regarding the application of age verification technology in the United Kingdom. While Child Wise does not have a view on such commentary, it does support the intent of the *Online Safety Act 2021 (Cth)* to develop Industry Standards to ensure reasonable and consistent application of such systems. In this context, Child Wise notes the following example cited by Yar (2019):

  "MindGeek, a company that owns a huge swathe of the most popular pornography sites, including Pornhub, Youporn, Redtube, tube8 and xtube. Pornhub alone accounts for more than 100bn video views per year, and its parent company reports annual revenues of $460m.

MindGeek's chosen age verification partner across all its services will be AgeID (www.ageid.com/) – which happens to be wholly owned by MindGeek itself."

- This raises further concerns regarding how platforms use of age verification will be monitored and enforced; "who checks the checker?" It would be a redundant process if it were left (in this example) for MindGeek to check themselves. Mechanisms for enforcement of the industry standards should be clearer.

Discussion Paper Question 7: Should the new RAS be prescriptive about the measures used to limit children's exposure to age inappropriate material, or should it allow for industry to determine the most effective methods?

Child Wise Response:

- Child Wise works directly with social media platforms and acknowledges that significant investment and effort is underway to ensure the safety of users and appropriateness of content.

- The potential for consistency across industry standards in age verification to facilitate access, monitoring and mediating of content, is a significant step to assist child-users, as well as their parents and guardians.

- Child Wise notes research by Pasquale, L., Zippo, P., Curley, C., O'Neill, B., & Mongiello, M. (2020) in a study commissioned by Cyber Safe Ireland, that documents the inconsistency in age verification across different platforms. For example:

Question	Snapchat	WhatsApp	Instagram	TikTok	Viber
1) What is the minimum age stated in the terms of use?	13	16	13	13	13
2) Is the minimum age the same across all EU countries?	Yes	16	No, in Spain is 14	Yes	Yes
3) Is it mandatory to input the age on sign-up?	Yes	No	Yes	Yes	Yes
4) If the answer to the previous question is yes, what happens if age 12 is entered?	Cannot create an account	N/A	Cannot create an account	Cannot create an account	Cannot enter age below 13
5) If you enter age 13, are there any additional verification processes?	No	N/A	Recommends to send an email to a parent	No	No
6) Is it possible to bypass the existing age verification process?	Yes, providing a false age	N/A	Yes, providing a false age	• Yes, providing a false age (2019) • No (2020)	Yes, providing a false age
7) If age 16 is entered on sign-up, is there any age verification process enabled?	No	N/A	No	No	No
8) At any point, is the minimum age made clear to the user?	Yes	Yes	Yes	Yes	Yes

Discussion Paper Question 8: Is there any additional information eSafety should consider in drafting a new Restricted Access System declaration?

Child Wise Response:

Consultation with children and young people

- Child Wise is unequivocal that meaningful engagement with children and young people is central to effective safeguarding. The issues outlined in the Discussion Paper and the Child Wise response will be of the upmost interest to, and have a significant impact on children, particularly adolescents. Consultation with children and young people about their experiences is therefore paramount to the development and implementation of the *Online Safety Act 2021 (Cth)*, as it is critical that they have a voice in decisions which impact their lives.

- Child Wise has extensive experience in facilitating the participation of children and young people, and is currently undertaking consultation with young people on their experience of social media. Further, Child Wise has existing collaborations and partnerships with national and international organisations that specialise in engaging children and young people to facilitate their participation in decisions which impact their lives, such as UK-based Mind of My Own. Child Wise would welcome further discussion with the eSafety Commissioner on the issue of consultation, engagement and participation.

Consideration of online gambling, loot boxes and skins

- Child Wise notes that the *Online Safety Act 2021 (Cth)* does not specifically address children's access to either online gambling or simulated gambling through online gaming.

- Child Wise notes and supports the report of the House of Representatives Standing Committee on Social Policy and Legal Affairs following its inquiry into age verification for online wagering and online pornography, *Protecting the age of innocence* (February 2020), which states:

    - *The clear and consistent message received by the Committee is that strong identity and age verification processes are necessary to prevent young people potentially developing problem gambling behaviours and addiction.*
    - *Consistent with the Committee's view in relation to online pornography, the Committee considers that it is reasonable to expect that customers wishing to open an online wagering account be required to verify that they are 18 years or over, and that this happen before they can engage in online wagering.*
    - *While gaming is not captured by the definition of wagering under the Interactive Gambling Act 2001 and was therefore outside the scope of the inquiry, in the course of the inquiry it came to the Committee's attention that there is concern in the community about children and young people being exposed to simulated gambling through 'loot boxes' in video games.*

- *The Committee shares this concern, and notes the potential for loot boxes to act as a gateway to problem gambling and associated harms later in life.*
- *Given their resemblance to gambling, the Committee considers that loot boxes and other simulated gambling elements in video games should be subject to appropriate age restrictions, including through the use of mandatory age verification.*

- Further, Child Wise notes that in its response to the House of Representatives Standing Committee on Social Policy and Legal Affairs, the Australian Government disappointingly:

  - Only supported **in principle** Recommendation 4 which recommended the introduction of a requirement that customers are not to use an online wagering service prior to verification of their age as 18 years or over.

  - Only **Noted** (as opposed to 'supported') Recommendation 5 which recommended that the Office of the eSafety Commissioner or other relevant government department report to the Australian Government on options for restricting access to loot boxes and other simulated gambling elements in computer and video games to adults aged 18 years or over, including through the use of mandatory age verification. The Government noted a 2018 Senate Environment and Communications Reference Committee Inquiry into gaming micro-transactions for chance-based items (loot boxes), which suggested that further research was required prior to developing an evidence-based regulatory approach to mitigate against harms caused by loot boxes in games.

- Child Wise is concerned that gambling and gaming have not been given sufficient consideration in the implementation of RAS, given their potential damage to a child's healthy development.

- In the context of gaming, Child Wise notes the definition used by Wardle (2019), who states:

  "This is particularly true within video games, which incorporate relatively new and emerging practices that replicate and reproduce gambling-like activities within this media.

  These practices include loot boxes, where players pay to 'open' a virtual box in the hope of it containing in-game items of significantly higher value than their original outlay, or the gambling or betting of 'skins' (decorative in-game items) through various mediums….

  This then facilitates a range of other actions for players, such as the betting or trading of skins, mainly on third party websites. Skins are virtual items earned or purchased within video games, which have their own value within the gaming community…"

- Child Wise also notes research by Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020) that states the following regarding the prevalence of loot boxes in games accessible to children:

  - *A total of 58.0% of the top games on the Google Play store contained loot boxes, 59.0% of the top iPhone games contained loot boxes and 36.0% of the top games on the Steam store contained loot boxes.*
  - *93.1% of the Android games that featured loot boxes and 94.9% of the iPhone games that featured loot boxes were deemed suitable for children aged 12+.*

- *Video game companies are currently not required to disclose to their customers that any game contains loot boxes prior to purchase.*
- *In the absence of suitable content descriptors, it seems difficult for parents and guardians to make an informed decision about the exposure of their children to this potential risk factor for problem gambling.*

- Further, Child Wise notes research by Shi, J., Colder Carras, M., Potenza, M. N., & Turner, N. E., (2021) which states:

  - *"A convergence of gambling and videogaming has implications for youth gambling. Limited or no age restrictions for online games such as free to-play slot machines may allow youth early opportunities to engage in gambling-like activities that may lead to gambling problems. Social casino games (SCGs) that involve virtual currency may lead to monetary gambling. Other videogaming-related features such as loot boxes and skins betting offer non-monetary rewards with in-game value that may also have monetary value. A convergence between gambling and videogaming platforms may facilitate behavioural involvement across networks and consoles, providing robust access to gambling-like activities."*

  - *"Videogames that include gambling-like features or free-to-play gambling-related games, like SCGs, vary with respect to age restrictions and their enforcement. Gambling-related games without monetary wagering typically do not fulfill legal criteria for gambling."*

We appreciate the opportunity to contribute to this important public debate.

We have included over leaf a citation list with information on the academic articles referenced in this submission.

Kind regards

Natalie Siegel-Brown
Child Wise Managing Director

12 September 2021

Citation List

- Fidan, M., Debbağ, M., & Fidan, B. (2021). Adolescents Like Instagram! From Secret Dangers to an Educational Model by its Use Motives and Features: An Analysis of Their Mind Maps. *Journal of Educational Technology Systems*, *49*(4), 501–531. https://doi.org/10.1177/0047239520985176
- Logrieco, G., Marchili, M. R., Roversi, M., & Villani, A. (2021). The paradox of tik tok anti-pro-anorexia videos: How social media can promote non-suicidal self-injury and anorexia. *International Journal of Environmental Research and Public Health*, *18*(3), 1–4. https://doi.org/10.3390/ijerph1803104
- Salzano, G., Passanisi, S., Pira, F., Sorrenti, L., La Monica, G., Pajno, G. B., Pecoraro, M., & Lombardo, F. (2021). Quarantine due to the COVID-19 pandemic from the perspective of adolescents: the crucial role of technology. *Italian Journal of Pediatrics*, *47*(1), 40–40. https://doi.org/10.1186/s13052-021-00997-7
- Pasquale, L., Zippo, P., Curley, C., O'Neill, B., & Mongiello, M. (2020). Digital Age of Consent and Age Verification: Can They Protect Children? *IEEE Software*, 0–0. https://doi.org/10.1109/MS.2020.3044872
- Shi, J., Colder Carras, M., Potenza, M. N., & Turner, N. E. (2021). A Perspective on Age Restrictions and Other Harm Reduction Approaches Targeting Youth Online Gambling, Considering Convergences of Gambling and Videogaming. *Frontiers in Psychiatry*, *11*, 601712–. https://doi.org/10.3389/fpsyt.2020.601712
- Wardle, H. (2019). The Same or Different? Convergence of Skin Gambling and Other Gambling Among Children. *Journal of Gambling Studies*, *35*(4), 1109–1125. https://doi.org/10.1007/s10899-019-09840-5
- Yar, M. (2019). Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. *Policing : an International Journal of Police Strategies & Management*, *43*(1), 183–197. https://doi.org/10.1108/PIJPSM-07-2019-0108
- Zendle, D., Meyer, R., Cairns, P., Waters, S., & Ballou, N. (2020). The prevalence of loot boxes in mobile and desktop games. *Addiction (Abingdon, England)*, *115*(9), 1768–1772. https://doi.org/10.1111/add.14973