PROTECTING CHILDREN FROM ONLINE GROOMING

Cross-cultural, qualitative and child-centred data to guide grooming prevention and response

Professor Amanda Third
Dr Ümit Kennedy
Dr Girish Lala
Dr Pavithra Rajan
Ms Shima Sardarabady
Ms Lilly Tatam

YOUNG & RESILIENT RESEARCH CENTRE
WESTERN SYDNEY UNIVERSITY
Safe Online
Save the Children

Safe Online

Is the only global investment vehicle dedicated to keeping children safe in the digital world. Through investing in innovation and bringing key actors together, Safe Online helps shape a digital world that is safe and empowering for all children and young people, everywhere. The Tech Coalition Safe Online Research Fund is a groundbreaking collaboration fuelling actionable research and uniting the tech industry with academia in a bold alliance to end online child sexual exploitation and abuse. Learn more: https://safeonline.global/tc-safe-online-research-fund/.

Western Sydney University

Western Sydney University is one of Australia's leading institutions. Ranked in the top 2% of universities in the world, it was named number one in the world for its social, ecological and economic impact in the Times Higher Education (THE) University Impact Rankings in 2022, 2023 and 2024. Western Sydney University is a world-class university with a growing international reach and reputation for academic excellence and impact-driven research.
For more information, please visit: https://www.westernsydney.edu.au/

The Young and Resilient Research Centre

Embraces an integrated mode of research and development, education, training, and enterprise to research and develop technology-based products, services and policies that strengthen the resilience of young people and their communities, enabling them to live well and participate fully in social and economic life. https://www.westernsydney.edu.au/young-and-resilient

Save the Children

Is the world's leading independent organisation for children. We believe every child deserves a future. We do whatever it takes – every day and in times of crisis – so children can fulfil their rights to a healthy start in life, the opportunity to learn and protection from harm, wherever they are. http://www.savethechildren.net/

Save the Children's Safe Digital Childhood initiative

Is a major global effort to support digital inclusion, protect children online and promote the mental health and wellbeing of the next generation of resilient digital citizens. The initiative includes partnering with schools, communities and tech leaders to break down barriers to digital inclusion by making sure the children with the fewest resources can access devices and connectivity; offering targeted digital literacy and citizenship programs; helping technology industry partners embed child-centric safeguards into their platforms; and empowering children to advocate for their rights in the digital world.
https://content.savethechildren.org/safe-digital-childhood/

Acknowledgements

First and foremost, we extend our deepest gratitude to the 604 children and young people from Australia, Finland, Philippines, Cambodia, Colombia, Kenya and South Africa who gave their time to share their views and experiences of online grooming with us. Their contributions, their creativity and their resilience have inspired us to do more to support a better future for them and the generations to come. We stand by them as allies in the fight against online grooming.

We thank Save the Children offices in Finland, Philippines, Cambodia, Colombia, Kenya and South Africa for assisting with data collection, co-analysis and shaping the report. Deep gratitude to all the facilitators from the seven countries that led the workshops. Thank you to: Farzana Chowdhury, Stephanie Hannah, Rose Lewis, Skye Tasker and Sarah Rammal from Australia; Mikko Ahtila, Paula Soini, Elina Porraslampi and Matti Mikkonen from Finland; Liz-Marié Basson, Kgahliso Ngwenya, Kgomotso Papo, Patiance Zhou, Johan Troskie, Vutlhari Mdungazi, Tiyani Mashimbye, and Basetsana Nchabeleng from South Africa. We would also like to thank the facilitators from Kenya and Colombia.

We have been delighted to have partnered with Save the Children at all stages of this project and to have learned from their policy, advocacy and child rights expertise. Thanks to Helen I'Anson, and John Zoltner for their ongoing guidance and expertise, and to Junli Zhai for her expert project management support throughout the project.

EXECUTIVE SUMMARY

Study Overview

In the aftermath of the pandemic, incidents of online grooming and child sexual and financial exploitation are at an all-time high (Thorn, 2022; Finklehor et al, 2024). While the number of children who have access to an online device continues to increase around the world, so does their risk of being harmed (Marwick et al., 2024).

While online child sexual exploitation and abuse (OCSEA) occurs at scale, across diverse settings and contexts, research exploring the issue generally involves participants from single geographic or cultural contexts. Moreover, existing research tends to focus on victim-perpetrator interactions, with the result that, internationally, there is little evidence to show how children – in all of their diversity – make decisions about who to engage with and why, as they navigate fast-paced, often socially-oriented, digital platforms and services. Cross-cultural data sets and analyses that document children's decision making in relation to engaging with unknown others are urgently needed to enable governments, businesses and NGOs to design effective strategies to mitigate the various forms of child exploitation that originate online.

With funding from the **Tech Coalition Safe Online Research Fund**, in 2023-24, **Save the Children** Hong Kong partnered with the **Young and Resilient Research Centre at Western Sydney University** and six Save the Children offices, primarily in the global South, to explore how children from diverse backgrounds experience the various pleasures and pressures of engaging with unknown others online, and what steps they take to protect themselves from potential harm. By listening carefully to children, the study aimed to identify how governments, technology platforms, services, educators, and parents might channel children's insights into the design of more effective policies, programming, product features, and systemic change to better support children to prevent, respond to, and report OCSEA.

To generate in-depth, granular insights into children's engagement with unknown others online, we deployed the Young and Resilient Research Centre (Y&R)'s unique distributed data generation methods (DDG). A primarily qualitative approach that configures children as partners in the research process, DDG entails in-country child-facing organisations – in this instance, Save the Children offices – co-designing creative and participatory workshops with Y&R and then implementing them with diverse children in multiple different cultural contexts simultaneously. Data is shared via a General Data Protection Regulation (GDPR)-compliant process with Y&R and co-analysed by Y&R and in-country partners using visual and discourse analysis techniques to ensure that analysis is faithful to cultural context.

?

In total, this project worked with 604 children aged 8–18 years in Colombia, South Africa, Kenya, the Philippines, Cambodia, Finland and Australia to explore the following questions:

- How do children in different contexts judge whether it is safe or unsafe to connect with an unknown other?
- What tools and strategies do they use to keep themselves safe? What tools and strategies do they use to keep themselves safe?
- To what extent do gender, age, and culture affect children's online engagements with unknown others?
- What might prompt children to report unwanted contact from unknown others online?
- What do children need from governments, technology platforms, NGOs, educators and parents to enable them to prevent or respond effectively to incidents of online grooming?

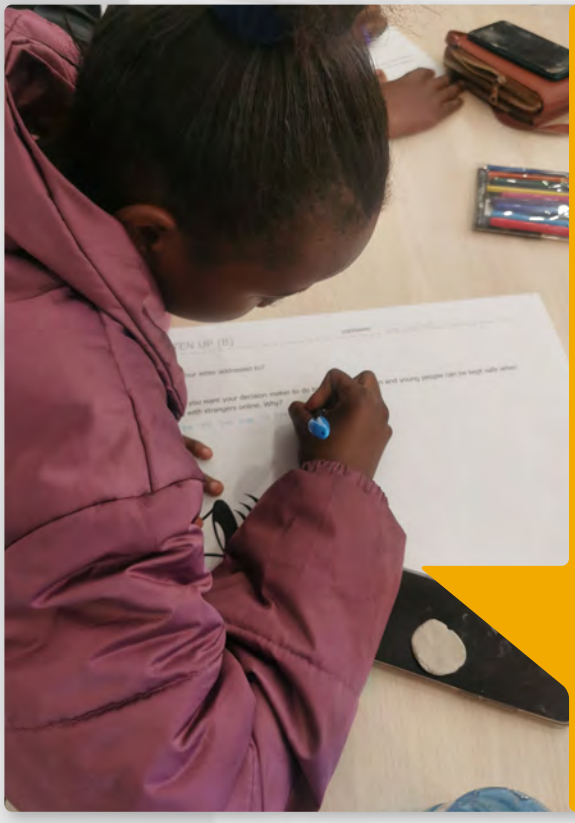
What did we learn from children?

1

Children routinely encounter unknown others in the spaces they congregate to socialise online.

Children primarily interact online with those they know in their face-to-face settings. However, they also routinely encounter unknown others in online spaces where they congregate to socialise with peers. Indeed, 66% of study participants interact with unknown others daily, predominantly via social media and gaming platforms. Online safety advice to avoid interacting with strangers online thus needs updating to address the reality of children's interactions online.

Children interact with three kinds of others online: a) Genuine Friends: those people they know face-to-face, including casual acquaintances; b) Known Unknowns: those they know of through their friends' and families' face-to-face and/or online social networks; and c) Unknown Unknowns: those they meet exclusively through online interactions. In general, children only fully trust Genuine Friends.



2

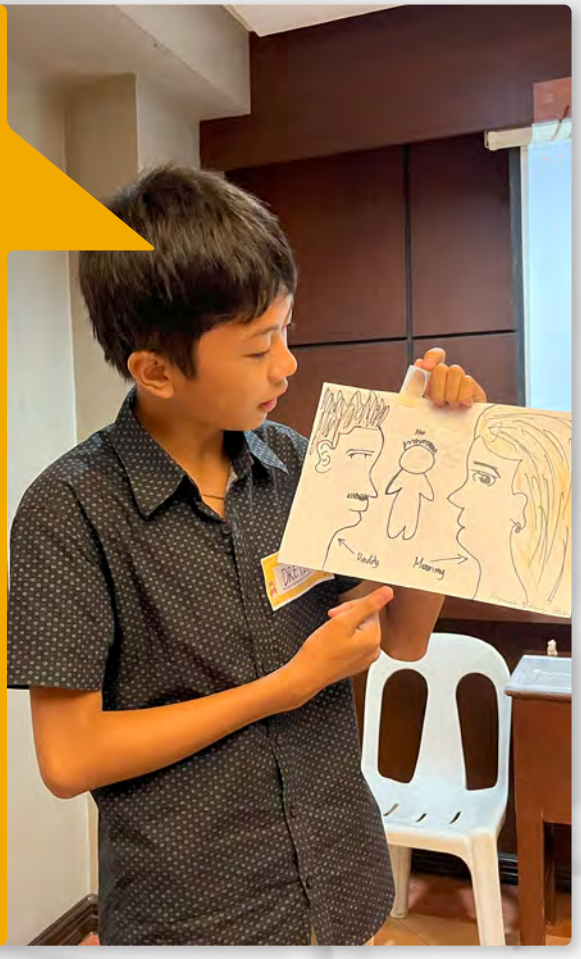
Children regard all those online connections they have not met face-to-face with a degree of suspicion

Children tend to treat online connections they do not know face-to-face – both Known Unknowns and Unknown Unknowns – with a degree of suspicion: 86% say they approach strangers online with caution. Children find it easier to assess the identities and intentions of unknown others in face-to-face over online settings. The risk of harm children associate with interacting with unknown others online depends on their context. Children in middle-income countries are more likely to consider unknown others online as a threat to their physical safety, compared with children in high-income countries, who often fail to see online others as a physical threat. This reminds us that young internet users form perceptions about the potential dangers of interacting with unknown others online through comparison with their experiences of safety in their face-to-face environments.

3

Children are motivated to interact with unknown others by a strong desire for friendship and to expand their networks and opportunities.

As they mature and become more social, children are more inclined to connect with unknown others online. Children are particularly curious about pursuing interactions with Known Unknowns. They are motivated to do so primarily by a genuine desire for friendship, fun and play, followed by a desire to stay informed about trends and events, to connect over shared interests, and to expand their networks. Concerningly, the potential to derive financial benefits is an incentive for children in middle-income countries to connect with unknown others online, potentially compromising their safety online. Children want adults in their lives to understand that engaging with unknown others is normal when engaging online and can be both enjoyable and beneficial, particularly for those who experience loneliness or who find it challenging to nurture face-to-face friendships. Children's interactions with unknown others may be short-lived or evolve into longer-term friendships, and they may stay online or eventually develop face-to-face dimensions.



4

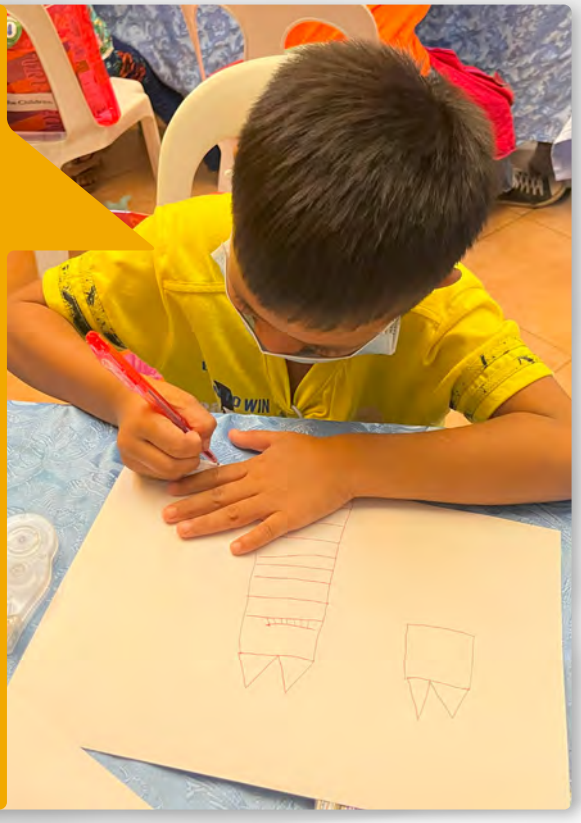
Children weigh up the risks of harm and the potential benefits when assessing whether to interact with unknown others online

Children generally know that engaging with unknown others online can be risky. They are concerned unknown others might expose them to online bullying; physical harm; inappropriate requests for personal information; data and privacy risks; inappropriate sexually-oriented exchanges; or criminal activities. Certain platform features exacerbate the potential to be harmed by unknown others online, including private messaging, geotagging , anonymity, and in-app purchases (Kuzma, 2012; Witzleb et al, 2020). Children also worry that consistent exposure to violent, sexually explicit and other age-inappropriate content can normalise inappropriate behaviours online and increase potential harm. Children in middle-income countries (63%) were more likely than those in high-income settings to report feeling afraid, anxious or uncomfortable when unknown others contact them. Importantly, being aware of the risks of harm rarely deters children from engaging with unknown others online.

5

Children use relational verification and targeted investigation strategies when interacting with unknown others online.

Children's existing networks function as a safe foundation from which they can explore relationships with Known Unknowns. They are much more likely to accept a friend request from someone they have seen or met in real life. Not having face-to-face contact or strong social reference points for new contacts tended to trigger negative feelings and greater levels of suspicion. Children's decision-making about interacting with unknown others is shaped by two ongoing practices: relational verification and targeted investigation. Relational verification involves scrutinising and evaluating whether unknown others have existing face-to-face or online connections with other trusted connections. Children's targeted investigation practices include conducting background checks, asking questions, or requesting proof of identity to determine if it is safe to engage with an unknown other online.



6

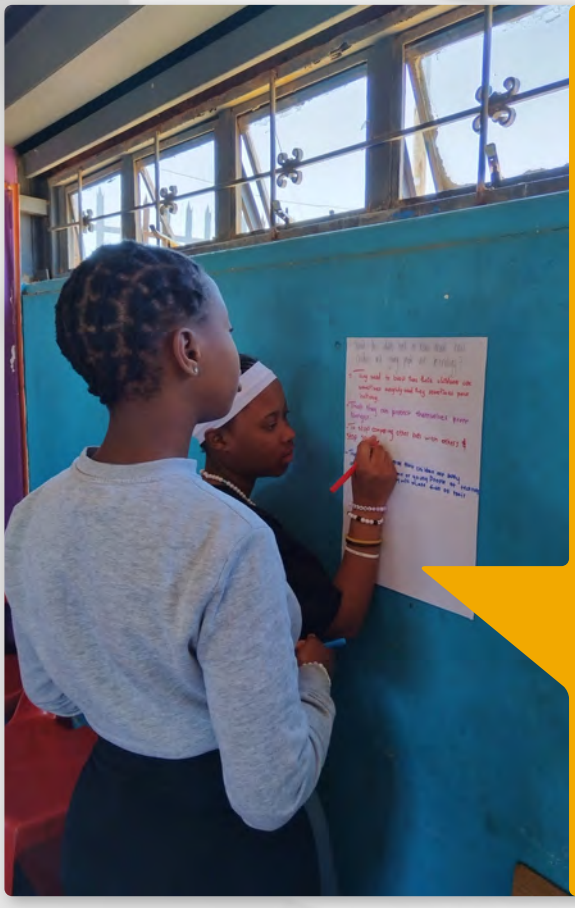
Children observe new online connections over time to determine their authenticity and to monitor whether they are trustworthy.

Far from blindly trusting unknown others online, children are constantly evaluating interactions, events, and behaviours to determine who is authentic and safe to engage with across online and offline spaces. They monitor unknown others' modes of online self-representation and behaviours towards others over time, looking for signs of authenticity to guide their decisions about whether to engage and to what extent an unknown other merits their trust. Children report that it is often difficult to ascertain the motives of unknown others. However, a series of red flags signal a contact cannot be trusted and, in some instances, are reason to block or delete contacts from their online friendship networks. Red flags include comments on their body or appearance; questions about where they live, go to school, or work; requests for personal information, such as date of birth or identity documents; and questions about their personal life, such as their relationship status.

7

Children prioritise protective strategies that are easy to implement inside the flow of their fast-paced digital media engagement

Children protect themselves from potentially harmful interactions with unknown others using a combination of preventive and responsive strategies. Their preventive strategies include restricting the personal information they share with unknown others; not accepting connection requests from unknown others; using privacy settings and strong passwords; and always being vigilant and careful. Children's responsive strategies include ignoring and rejecting requests, blocking and reporting, responding to unknown others by asking them to stop, asking questions, changing topic and ultimately disconnecting from the platform and device. Children tend to mobilise responsive strategies that are easy, routine, accessible and which do not require them to step outside the flow of their digital media activities. Not surprisingly, then, the most common protective strategy used by children is to ignore unwanted contact from unknown others online, which prevents further interaction. A total of 82% of participants found it easy to block unknown others online, and older children found it significantly easier to block people than younger children.



8

Children experience significant barriers to reporting online grooming incidents

Children believe that formal reporting mechanisms are a key to a robust online safety ecology. However, while they assert the value and relative ease of formal reporting processes, many are nonetheless reluctant to report unknown others through formal channels. It appears that the barriers to reporting are primarily attitudinal and differ across cultural contexts. Our analysis suggests that reporting is thus regarded as a 'serious' step and a sign that a situation has significantly escalated. Formal reporting often requires children to step outside the flow and familiarity of their routine digital practices into a process that is often opaque to them. They are not always sure what reporting processes entail and whether they are confidential. Nor do they always know what happens to their report once they lodge it, who looks at it, how it is assessed, and what kinds of actions might ensue. For these reasons, they are much more likely to report an incident to a friend (80%) than to the platform (54%) or to an authority (54%). In middle-income countries, in particular, children reported a reluctance to report to authorities such as police.

9

Children regard their online safety as a responsibility shared by government, NGOs, technology platforms and their broader communities

Children assert that their online safety is a whole-of-community responsibility. They highlight the important role of parents and caregivers, governments, technology companies, and schools to keep them and their peers safe online. Children urge governments to work with and direct industry to provide protections against harmful users and accessible mechanisms to respond and report potentially harmful experiences. They urge governing bodies and decision makers to consider ways to ensure that their digital participation is age-appropriate – for example, by designing and enforcing rules that mandate age restrictions for social media use, regulate online content, or limit access to devices by age. Children call for legal systems to be strengthened to facilitate justice for those who experience online grooming, and for police to increase security around community internet facilities, such as internet cafés, kiosks, and pisonets . Children say, above all else, they need parents and other family members to supervise their digital practices, and to establish and enforce clear and rigorous rules to protect them online.

10

Children want clear avenues for guidance and support to strengthen their online interactions

Where children go to for help and advice about online safety is heavily dependent on who they trust – and therefore differs according to geographic, cultural, political, and social context. Children from high-income countries are more likely to seek help from formal structures of support, such as services, helplines and police or other authorities, while those in middle-income countries are more likely to seek out community structures of support, such as community leaders, community elders, and community organisations. Across countries, children's number one source of help and guidance is a trusted adult –usually a parent or guardian – followed by their friends, NGOs, counselling services, and child protection services. Very few children said they would be confident about turning to teachers or police, due to fear of being misunderstood or punished, or because they are unsure about the confidentiality of seeking help via these avenues.

11

Children want to turn to parents and caregivers for support but feel they are underequipped to guide their children

Children believe that skilling parents and caregivers needs to be a key focus for future online safety efforts. In their experience, parents and caregivers do not understand the dangers children face online and/or lack knowledge and confidence about how best to support, guide, or respond to potential online risks and harms. Children feel parents and caregivers are also insufficiently appreciative of the benefits of online contact and communication. Children want their parents and caregivers to understand the platforms they use, who they interact with, what they share, and how they might be harmed online, and they call for education targeting trusted adults. Children suggest that such education should teach parents and caregivers about the benefits of their digital technology use; how to support children to avoid potentially harmful behaviours; how to respond to strangers; what content is appropriate to share; and how to block and report inappropriate behaviour.

12

Children are calling for widespread, accessible and targeted education about safe interaction with unknown others online

Across countries, children highlight an urgent need for online safety education to be accessible to every child across the developmental stages of childhood and adolescence, regardless of where they live. They call specifically for education about methods to identify risk online; what information is appropriate to share online; how to appropriately respond to unknown people; where they can go when they need help; and how to report inappropriate behaviour online. Children want educational initiatives to take place in accessible and familiar contexts, within schools and communities, as well as online platforms, apps and games. They call for platform- and site-based education to leverage popular digital formats, such as video, to deliver online safety information. Children say that governments and technology companies should partner to develop, activate, and deliver education programmes, not only to all children, but also to all adults.

13

Children believe technical innovations can profoundly improve their online safety

Children are alert to the potential for technical capabilities to be leveraged to strengthen their online safety. In particular, they urge companies to use artificial intelligence to improve the discovery of online safety information, education, and tools; to implement automatic blocking and banning; to increase the security of personal information; and to ensure interactions are age-appropriate. Children urge technology platforms to use algorithmic tools to target online safety information and education to best effect and to better immerse online safety information and features in the platforms, apps, and games they use. Children want technology platforms to consider implementing additional mechanisms to protect their data; to prevent their inadvertent contact with ill-intentioned adults; and to minimise their exposure to age-inappropriate content. Children also suggest default privacy settings for minors; automated warning systems to alert them when they interact with someone whose intentions may not be genuine; AI-powered, appropriate, relatable, just-in-time guidance about possible and safe responses, to help them decide if or how they will engage with unknown others; and automated blocking and reporting processes for young users. Children want safe online spaces to discuss or report potentially harmful behaviours and content. They want companies to better communicate how reporting and other online safety processes work; to be confident about the outcomes of reporting; and to be told when and how community guidelines are enforced.

RECOMMENDATIONS

1. Better support children to manage their relationships with friends and a range of unknown others online, including those with whom they have a mutual connection and those who are completely unknown to them.

2. Encourage children and the adults who support them to block and report bad actors online.

3. Strengthen pathways to support services to support young users to address online grooming and other online safety challenges.

4. Strengthen and increase the accessibility of online safety and digital literacy education for children, regardless of location or age, to support their management of interactions with unknown others.

5. Strengthen education for parents, carers, teachers, and community leaders to equip them to better communicate with and support their children to interact safely with unknown others.

6. Equip decision-makers to take informed decisions about how to strengthen responses to online grooming.

7

Strengthen and enforce legislation and mechanisms of justice for children who experience online harms.

8

Consider developing a default industry standard around online privacy and security by default for children to minimise the possibility that they inadvertently share personal information with bad actors in ways that compromise them.

9

Reduce the likelihood that children will encounter violent, sexually explicit, or other age-inappropriate online content.

10

Reduce the likelihood that children will unwittingly interact with adults and those who might be bad actors in online spaces, and ensure that children can engage in age-appropriate interactions.

11

Consider implementing AI-driven warning systems to alert young users about the characteristics and prior practices of unknown others with whom they interact online.

12

Ensure platform features do not exacerbate the risk that children might be exposed to bad actors online.