



Netsafe submission to the Parliamentary Inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in addressing those harms

Summary

Netsafe welcomes this Inquiry as a vital opportunity to strengthen online safety for children and young people in Aotearoa. Our evidence shows that online harms are increasing and evolving, particularly cyberbullying, sextortion, scams, and exposure to distressing harmful or illegal content.

While proposals like restricting access to social media for under-16s reflect genuine concern, a one-size-fits-all response is unlikely to be effective and risks driving harm underground. A ban or restriction on its own won't address the scale or complexity of the issues and may give a false sense of security.

Instead, Netsafe proposes a comprehensive, future-focused strategy to:

- **Modernise regulation and drive platform accountability:** by introducing clear platform responsibilities such as requiring safer design features.
- **Invest in digital education:** by scaling up age-appropriate, curriculum-integrated digital literacy and online safety education from early childhood to secondary school.
- **Support parents and teachers:** by providing practical resources to help adults guide and protect children online.
- **Fund wraparound support:** to ensure wellbeing services are available to address the real-world impacts of online harm.
- **Work globally:** by collaborating with other like-minded governments and organisations to ensure a coherent and effective approach and to raise global safety standards.

Netsafe stands ready to support Parliament in crafting an evidence-based, proportionate, and child-centred approach that reflects how young people actually experience the online world and delivers real change.

1. About Netsafe

- 1.1. Netsafe is New Zealand's independent, non-profit online safety charity operating for over 25 years. Our foundations lie in education. Netsafe provides free support, advice and education to all New Zealanders seven days a week through a helpline, our website and face to face service delivery across New Zealand. We work adjacent to Government and law enforcement, and are supported and funded by the public and private sector. Taking a technology-positive approach to the challenges digital technology presents, we work to help people in New Zealand take advantage of the opportunities available through the internet by providing practical tools, support and advice for managing online challenges.
- 1.2. Netsafe is also the Approved Agency under the Harmful Digital Communications Act 2015 (HDCA) (a role to which we were appointed in 2016 and renewed in 2021 until June 2026). One of the purposes of the HDCA is to deter, prevent, and mitigate harm caused to individuals by digital communications. Netsafe's functions as the Approved Agency are set out in section 8 of the HDCA. Those functions include:
 - a) to receive and assess complaints about harm caused to individuals by digital communications
 - b) to investigate complaints
 - c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints
 - d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of the Act
 - e) to provide education and advice on policies for online safety and conduct on the Internet.
- 1.3. The HDCA and the Approved Agency offers civil and alternative pathways to the criminal justice system, which is particularly important for youth involved in online harms and restorative outcomes.
- 1.4. In addition to our long-standing leadership in online safety, Netsafe is currently integrating the nationally recognised youth charity Sticks N Stones into our operations. This strategic merger strengthens our expertise in youth-led and peer-informed cyberbullying prevention, further enhancing our ability to respond to the needs of rangatahi across Aotearoa.
- 1.5. Netsafe's submission reflects our extensive frontline experience addressing online harms -as both a not-for-profit agency and in our statutory role as the Approved Agency under the Harmful Digital Communications Act. And also through our extensive partnerships and relationships which include:

- 1.5.1. Our standing youth advisory panel the Youth Action Squad¹ which empowers rangatahi across Aotearoa to contribute to Netsafe’s thinking and projects, plan their own initiatives, lead campaign activities, and enact change in their local communities.
 - 1.5.2. Collaboration with the Online Safety Iwi Leaders Group under Pou Tangata of the National Iwi Chairs Forum
 - 1.5.3. Our observer status on the Global Online Safety Regulators Network, Chair of the Oceania Global Anti-scams Alliance and relationships and projects with a number of other organisations based outside New Zealand.
 - 1.5.4. Our trusted flagger status with a number of the major online platforms.
 - 1.5.5. Our role as the New Zealand hotline for INHOPE² to ensure the rapid identification and removal of Child Sexual Abuse Material from the internet; and
 - 1.5.6. Work we undertook to stand up the Aotearoa New Zealand Code of Practice for Online Safety and Harms³ (in the absence of any Government action).
- 1.6. Netsafe acknowledges and supports many like-minded organisations that seek to be data led and evidenced based in their submissions to this inquiry. We believe strongly in the importance of coordinated efforts to improve online safety outcomes for children and young people. We encourage the Committee to give particular consideration to proposals that reflect New Zealand's online experiences, are evidenced based and align with the work of trusted organisations such as Youthline, Save the Children, the Office of the Children’s Commissioner, Save the Children New Zealand, Te Ata Hāpara and Pou Tangata of the National Iwi Chairs Forum. These bodies offer valuable youth, frontline, community, and rights-based perspectives which should be reflected in any recommendations that may emerge.

2. What Netsafe’s data tells us

- 2.1. There is no question that both adults and children alike continue to experience harm online. Over the past four years (2021-2025), Netsafe’s data reveals a persistent and growing pattern of reported online harm affecting adults, children and young people across New Zealand. Cyberbullying and harassment continue to be the most commonly reported issues, with young people aged 13 to 17 representing an increasingly large share of complaints received by Netsafe.⁴⁵

¹ See more about Netsafe’s Youth Action Squad here: <https://netsafe.org.nz/our-work/youth-action-squad>

² <https://inhope.org/EN/our-story>

³ <https://thecode.org.nz> The Code is now administered by NZTech.

⁴ See Netsafe Annual Reports here: <https://netsafe.org.nz/our-work/reports-and-research>

⁵ See also *Cyberbullying in New Zealand: \$1b cost in 2023*

<https://cdn.sanity.io/files/8y8wsx0z/production/2ccc1324a82b6ae2a70c8167b0b896240b7755c3.pdf>

- 2.2. Sextortion and image-based abuse have seen a dramatic surge, with Netsafe recording an overall 88% rise since 2019. Scams and phishing attempts are also escalating sharply; in our 2024 Annual Report, we reported scam losses totalling \$17.8 million, highlighting the growing targeting of young people and families through social media-based and impersonation scams.⁶
- 2.3. Exposure to harmful, offensive or age restricted content including violence, terrorism or extremism, self-harm and pornography remains widespread among youth. Earlier surveys indicated nearly half of all young people have encountered such content.⁷
- 2.4. The COVID-19 pandemic also contributed to a sharp rise in online harms, and post-pandemic levels of harm remain significantly above 2019 baselines. High volumes of reports continue across key categories including cyberbullying, sextortion, and scams.
- 2.5. Other research, such as that we undertook in partnership with Te Mana Whakaatu – the Classifications Office on body image,⁸ shows the potentially negative effects social media and online content may have on children and young people’s own appearance, fitness and self worth.
- 2.6. More recent research that Netsafe undertook with Save the Children, asked children and young people to share their views, experience and advice related to online safety, providing valuable youth insights.⁹
- 2.7. We also know there is significant unmet demand for education and educational resources. The rapid uptake of new and updated resources illustrates both the urgency of the need and the willingness of educators to engage. For example, the 2024 relaunch of *Hector’s World*,¹⁰ Netsafe’s foundational online safety resource for children under 12, has already reached families through more than 162,000 video views and 26,000 website visits. This reflects strong demand at the critical pre-social media age when online activity begins through gaming and video platforms. More than 4,000 registered teachers from hundreds of schools have accessed Netsafe’s educator portal, alongside 40 Life Education Trust teachers now delivering the programme nationwide. And at the intermediate and

⁶ Netsafe Year in Review 2023/24

<https://cdn.sanity.io/files/8y8wsx0z/production/c10b42b2a96a1c96ed33633e7f6f2d3f226e1f29.pdf>

⁷ *New Zealand children’s experiences of online risks and their perceptions of harm*

<https://cdn.sanity.io/files/8y8wsx0z/production/aae93d71583f725fa4f84325faf233b22aff25a2.pdf>

⁸ *Digital Reflections: The Online Experience and its Influence on Youth Body Image in Aotearoa*

<https://cdn.sanity.io/files/8y8wsx0z/production/5e5a46c8e335c3b838e13081a7035234c0b23249.pdf>

⁹ *Report: Children and Youth Online Safety in Aotearoa New Zealand*

<https://cdn.sanity.io/files/8y8wsx0z/production/cdaa8f37aa4ca375042375f1ab74d5e9dd36403a.pdf>

¹⁰ <https://www.hectorsworld.com>

secondary level, our new education platform saw over 35,000 resource downloads and nearly 10,000 student module completions in the last year alone, with 1,290 schools, (around 75% of all secondary schools) now engaged.

- 2.8. These figures point to the scale of work already underway, but also to the growing gap between demand and available support. Insights from our 2025 research with teachers (unpublished) reinforce this: despite the cell phone bans in schools, teachers continued to identify cyberbullying as the most common incident affecting schools (70%), followed by exposure to distressing content, sextortion, and unsafe platform use. Teachers also report that students continue to lack understanding in key areas such as online risks (e.g. scams, sextortion); privacy and digital footprint; media literacy and algorithmic influence. The appetite for preventative, relevant, and trusted resources is strong, but current capacity falls short of what is needed to meet the scale and complexity of online harm facing young people today.
- 2.9. Finally, the rapid emergence of AI-enabled threats, such as deepfake abuse, synthetic image creation, and impersonation scams, introduces new risks. These technologies can target young people even if they have never shared private content, creating complex challenges for online safety.
- 2.10. As can be seen from the above there are different types of harm potentially experienced, each with their own potential cause or causes, and their own potential solutions.

3. How did we get here?

- 3.1. New Zealand's approach to regulating digital content and digital platforms is fragmented and inconsistent. While there are strong elements within our current framework, such as the Harmful Digital Communications Act 2015, the broader regulatory system does not function coherently or effectively. Gaps remain in how we regulate content, hold platforms accountable, and support those affected by online harm whether through redress mechanisms or education. For example, while the Department of Internal Affairs has policy responsibility for digital safety, the Ministry of Education is responsible for digital safety education in schools, the Ministry of Justice is responsible for Harmful Digital Communications Act policy, the Ministry of Business, Innovation and Employment is responsible for scams policy and the Ministry of Health determines policy settings around mental health and wellbeing. Online content is variously regulated through the criminal law, through New Zealand's objectionable content regime administered by Te Mana Whakaatu – the Classifications Office, the Broadcasting Standards regime, voluntary industry bodies such as the Media Council or not at all.

- 3.2. At the same time, as technology use has increased we have placed children in a contradictory and complex digital environment. Device use is more often than not compulsory in many schools, and drivers such as the COVID-19 pandemic pushed life further online - online platforms became essential for education and maintaining social connections. Children are now exposed to digital environments at increasingly younger ages. The use of technology is not only embedded in our education and social infrastructure, but also widely accepted and modelled by adults.
- 3.3. We have not adequately invested in or funded digital safety prevention, response and policy work. There has been the net loss of 22 digital safety roles at the Department of Internal Affairs, a significant downsizing of the digital safety function and the loss of the Government's Chief Privacy Officer function. Investment in baseline digital safety education has remained static. As an example, Netsafe receives \$816,000 per year under contract from the Ministry of Education to support every school with online safety education, advice and response¹¹ which does not keep pace with the increase in online safety incidents and digital safety education needs. And digital safety does not feature in the national school curriculum in any meaningful way.
- 3.4. We are also witnessing broader societal change including declining social cohesion.¹² So some of the challenges associated with online life could have deeper roots in societal shifts. That's why Netsafe supports this inquiry, not just to examine online harms in isolation, but to explore these issues in a comprehensive and systematic way.
- 3.5. This is a nuanced issue, with different views and complex considerations. Research in this area is often contradictory or inconclusive, and it is difficult to establish causation rather than correlation. We are also aware of the ethical constraints on conducting research with young people but it is important that adult centred research is not used in place of the youth experience. If the evidence base is incomplete or unclear, this should trigger further research. Policy decisions of this scale and impact should be based on insight, not intuition.
- 3.6. Globally, no country has yet found the perfect solution. Nevertheless, we have an opportunity to learn from global developments and to craft an approach that reflects the New Zealand context.

¹¹ There are more than 2,500 primary and secondary schools and 850,999 students according to figure.nz and Ministry of Education July 2024 data. This funding equates to less than \$1 per student p.a.

¹² *Social Cohesion in New Zealand* <https://helenclark.foundation/publications-and-medias/social-cohesion-in-new-zealand/>

4. Why broadbrush proposals are not the silver bullet

- 4.1. Netsafe fully supports the goal of enhancing online safety for children and young people and is aligned with those advocating for stronger protections. However we strongly caution against one-dimensional solutions to multidimensional problems. The risks children face online are real and pressing. But the response must be comprehensive, future-facing, informed by evidence and must avoid unintended consequences. Root causes such as poor platform design, insufficient or ineffective regulation, a lack of sustained support for digital education, and gaps in support systems must be addressed in ways that are proportionate and enduring, and which do not restrict fundamental rights or access to technologies that also offer connection, creativity, and learning.
- 4.2. While the proposal to ban or restrict social media for young people has prompted long overdue debate, focussing on what looks like a quick win has the potential to create significant unintended consequences and to simply shift the problems elsewhere.
- 4.3. The aims for such a ban outlined e.g. in Catherine Wedd MP's Private Members Social Media (Age Restricted Users) Bill are commendable: The stated policy aims of that Bill are to:
 - reduce the risks to young people of cyberbullying, harmful content, and online exploitation
 - safeguard young users' privacy from commercial exploitation and data breaches
 - encourage healthier social interactions and offline activities
- 4.4. However, a closer examination reveals that the Bill as proposed is unlikely to deliver on these objectives.
- 4.5. First, cyberbullying will not be solved by simply restricting children from social media. Our research shows that cyberbullying behaviours migrate to other digital spaces such as gaming platforms or messaging apps.¹³ It is therefore more important to focus on the underlying root causes of bullying if the aim of reducing bullying is to be achieved. A more effective and proportionate approach would include targeted anti-bullying education, resilience-building programs, and increased support systems.
- 4.6. Second, while seeking to restrict access to social media might reduce children's exposure (intended or unintended) to certain harmful content hosted on social media platforms, it would not stop access to harmful content distributed through other channels, including peer-to-peer sharing or other websites or accessed by way of VPNs. Harmful content is not confined to social media, and limiting access to one type of platform does not

¹³ Insights from research Netsafe conducted with teachers in 2025 (unpublished).

guarantee overall protection. In addition, “harmful” content would need to be clearly defined and categorised given each type of potentially harmful content carries with it specific risks or consequences. Seeking to address all “harmful” content under a single banner and in the same way is unlikely to be an effective and proportionate means of achieving the aim of addressing the particular effects of that content. Take, for example, access or exposure to pornography or other age restricted content. It is difficult to see how banning or removing access to social media platforms for under 16 year olds achieves the aim of preventing access or exposure to such content (which is more likely to be hosted or found off social media platforms) for anyone under 18. The point here is that each potential harm may need a different solution.

- 4.7. Third, the objective of safeguarding young users’ privacy from commercial exploitation or data breaches is unlikely to be achieved through a social media ban alone. Children remain online through various other platforms and services or parental sharing, so the core privacy risks persist regardless of access to social media specifically.
- 4.8. Finally, the aim of encouraging healthier social interactions and offline activities is difficult to realise through a restriction on social media use. Unless children were prohibited from going online altogether, which is neither realistic nor desirable, simply banning social media does not guarantee increased offline engagement or healthier social behaviours.

5. Unintended consequences

- 5.1. Netsafe is also concerned that a blanket social media restriction for children under 16 carries a significant risk of unintended consequences that could undermine the very aims it seeks to achieve. The reality is that digital behaviour does not simply disappear when access is restricted. It adapts, migrates, and often becomes harder to detect and manage.
- 5.2. We have already seen this pattern play out in practice. The recent ban on cell phone use during school hours was implemented with the intention of improving learning, wellbeing and reducing distractions. However, there is as yet, no compelling evidence that that ban (here or internationally) has meaningfully reduced cyberbullying among students. In fact, the bullying behaviour has largely shifted to less visible platforms such as SMS, shared school documents, or gaming chat functions where it can be harder for adults to monitor. The cyberbullying problem has not been solved; it has simply changed form and location.¹⁴

¹⁴ Insights from research we conducted with teachers in 2025 (unpublished): Despite the phone ban, cyberbullying (70%) was the most common incident affecting schools. We also know qualitatively from teachers for example, that

- 5.3. Of more concern is that the cell phone ban in schools appears to have shifted responsibility from schools to homes.¹⁵ When issues arise on platforms outside the school environment, the ability of schools to intervene becomes limited, and parents and caregivers are left to manage complex interactions with little support. This kind of displacement effect clearly needs more research and highlights that without careful design problems may be forced underground or into even less regulated spaces.
- 5.4. We could also predict that banning children from one type of technology or platform will simply shift them elsewhere. One such space is the rapidly growing domain of AI companions that simulate human interaction and present as “friends,” “partners,” or “confidants.” These tools are not currently classified as “social media” under most legal definitions. Yet, they pose risks that are in many ways more complex and less understood than traditional social media platforms. Unlike public social media platforms, these AI tools often operate outside mainstream visibility, without the same content moderation systems or oversight mechanisms in place.
- 5.5. If the intent of a ban is to reduce harm, enhance privacy, and foster healthier development, then the scope would need to include these emerging technologies too. And if we ban AI companions, what about online gaming? What about online content or activity not captured by the definition of social media?
- 5.6. This underscores the broader risk of legislating in a way that is reactive rather than reflective. By focusing narrowly on a single category of technology we risk ignoring the evolving nature of digital life and the many other platforms children and young people engage with daily. Without a future-focused approach, we are likely to repeat past mistakes by addressing symptoms in one environment while ignoring their reappearance in another.
- 5.7. We also need to ensure that technology companies do not avoid the level of accountability that is needed. Without parallel action to regulate design practices, enforce minimum safety standards, and ensure effective age-appropriate moderation, a ban simply sidesteps the platforms’ ongoing obligations to their users. These companies shape the digital spaces that children inhabit every day. Solutions that do not require them to change how those spaces ultimately fall short of ensuring real safety online.

the phone ban in schools simply moved behaviour to school endorsed platforms like Google. For these we are now being asked to create additional education resources.

¹⁵ We know this because our reports from schools managing incidents as a "school incident" have dropped, but the number of incidents reported to us "involving school aged children" has remained consistent - the fallout is being managed by parents.

- 5.8. Similarly, a ban may signal to the public that the Government's role in addressing online harm is complete. But this is not the case. On its own, a ban would be entirely insufficient. Significant additional action would still be required.
- 5.9. It also risks creating unrealistic expectations for families. Parents and caregivers will still need to play an active role in their children's online lives whether or not those children are officially allowed to access social media. Even with a ban, they will be left to monitor alternative platforms, manage conflicts, guide safe behaviours, and educate their children in an environment that continues to evolve rapidly.
- 5.10. Enhancing children's online safety requires navigating complex trade-offs between competing rights and interests. Measures such as mandatory age verification would help restrict access to harmful content, but they also compromise the privacy and anonymity of all internet users, including children, by requiring the collection of sensitive personal information, expanding surveillance or subjecting users to potentially biased AI systems. Such measures can disproportionately impact marginalised groups and deter legitimate online activity.

6. Potential solutions

- 6.1. Netsafe instead advocates for a more comprehensive strategy that acknowledges how children and young people actually use technology, is informed by youth voices and builds safeguards, skills, and support structures across the full digital ecosystem.
- 6.2. Importantly, any proposed approach must recognise that children are not a homogeneous group. Age, developmental stage, digital experience, and vulnerability all shape how a young person engages with technology. A uniform, one-size-fits-all approach that applies equally to a 5-year-old and a 15-year-old risks being both ineffective and inappropriate. This is why digital safety policy should be developmentally informed, reflecting a child's growing capacity for critical thinking, decision-making, and risk management.
- 6.3. A modern, forward-looking approach should include:

Greater coherence across government and public policy and multi-stakeholder collaboration and accountability

- 6.4. A more coherent, joined-up approach involving all relevant actors in New Zealand is needed - one that provides clear leadership, strategic coordination, and public accountability for outcomes. Netsafe is agnostic on whether this should be achieved by

the creation of e.g. a regulator or whether this could be achieved by an overhaul of policy responsibility within Government.

- 6.5. Online safety is a shared responsibility. A successful and sustainable approach will involve collaboration between government, industry, civil society, academia, educators, caregivers, and young people themselves. Formal multi-stakeholder bodies can help design better, more inclusive policy, ensure that lived experience and youth voice are embedded in decision-making, and create a shared sense of responsibility and transparency in how online safety goals are delivered and monitored.
- 6.6. New Zealand also needs a modernised legislative base and a coherent system to deliver on it. Other policy interventions including bans will remain isolated, reactive, and incomplete without this. As part of this there is an urgent need to review and modernise the Harmful Digital Communications Act. When introduced in 2015, the HDCA was world-leading, but the digital environment has changed dramatically in the decade since. A revised HDCA could better reflect the scale, complexity, and technological realities of current online platforms, including the emergence of AI-generated content, encrypted communications, group harm and synthetic media. It could also introduce proactive duties of care for platforms, streamline redress mechanisms, enable code making and enforcement functions and strengthen alignment with international online safety standards.

Stronger platform accountability and safer design standards

- 6.7. Central to any serious attempt to protect children online is the need for platforms to be made meaningfully accountable for the environments they create. Digital platforms must also be required to build safety into the design of their services from the outset or modify existing products to include safety features. This includes:
 - 6.7.1. Default privacy and safety settings for young users.
 - 6.7.2. Limitations on algorithmic amplification of harmful or illegal content.
 - 6.7.3. Rapid and accessible reporting systems with meaningful redress.
 - 6.7.4. Significantly increased proactive and preventative moderation to remove harmful or illegal content before it can be seen, including human moderation capacity that is responsive to New Zealand's legal and cultural context.
 - 6.7.5. Prevention of addictive or manipulative design features, such as infinite scroll or autoplay.

Expanded digital literacy and resilience education

- 6.8. Educating children and young people to navigate online risks is a known, important and effective harm prevention strategy. Digital literacy should be taught systematically across

the curriculum from early child education, primary through to secondary school and should include media literacy, critical thinking, online ethics, identity and privacy, digital wellbeing, and strategies for dealing with conflict, conduct or inappropriate content. Programmes should be tailored to reflect the real online lives of children, and co-designed with young people to ensure relevance and effectiveness.

- 6.9. Resilience-based education can also help young people cope with and recover from harmful online experiences. Children who are confident, informed, and supported are far better equipped to respond to digital challenges in a safe and constructive way.

Improved support and education for parents and caregivers

- 6.10. Children do not navigate the digital world alone. Parents and caregivers play a critical role in shaping how young people engage with technology but many feel unprepared to guide their children through the complexities of online life.¹⁶ Practical, accessible resources and community-based initiatives are needed to build parental confidence, strengthen communication within families, and provide clear guidance on managing devices, boundaries, and risks. Without supporting parents, no policy aimed at protecting children will be fully effective.

Increased funding for wraparound support services

- 6.11. Online harms often do not stay online. The effects, whether emotional, psychological, reputational, or relational, can spill into school life, home life, and mental health. Services that deal with these impacts, including counselling, youth wellbeing support, family violence services and addiction recovery, are chronically underfunded. If we are serious about reducing harm, Government must direct more consistent, long-term investment into these services. Funding should also support cross-sector collaboration, so that children can be referred and supported seamlessly across education, health, and justice systems.

Global cooperation and standard setting

- 6.12. Addressing the online harms experienced by children demands coordinated global action and robust international standard setting. These harms transcend national borders and are largely driven by the practices and products of a small number of powerful technology companies whose reach spans jurisdictions. While national responses remain important, they are insufficient in isolation. Disjointed or go-it-alone approaches risk fragmenting efforts and diluting overall effectiveness. Without global cooperation,

¹⁶ Parents have told us this in Netsafe's outreach and engagement events.

attempts to enforce safety standards, ensure responsible platform design, and uphold children's rights will continue to be undermined. It is imperative that governments work together to demand greater transparency, accountability, and safety-by-design from the tech sector. New Zealand must be an active contributor to these efforts, ensuring that Māori perspectives, rights, and aspirations, particularly those of tamariki and rangatahi Māori, are embedded in both domestic and international approaches.

- 6.13. New Zealand can also learn from overseas approaches. Several other jurisdictions including Australia, the United Kingdom, and certain U.S. states are currently trialling or considering regulatory measures aimed at restricting children's access to social media or requiring platforms to implement age assurance technologies. While these developments are notable, many are still in their early stages. Australia is still grappling with what is in or out of its own social media ban.¹⁷ And we can already see for example the UK's age-gating requirements have promoted a huge surge in VPN uptake and use, which if it continues at the current rates would significantly undermine the objectives the age-gating requirements seek to achieve.¹⁸ Before New Zealand replicates such measures wholesale we should fully understand how effective they are, what unintended consequences they produce, and what lessons can be drawn from their implementation.

Measures required even if a ban were implemented

- 6.14. If a ban or restriction on social media for under-16s were nevertheless implemented, it would be vital to recognise that the alternatives outlined above are not optional. A ban would not resolve the complexity of online harm on its own and would still need to be part of a broader, well-resourced online safety strategy including all of the above measures and noting in particular that:
- 6.14.1. If children are to be restricted from certain technologies, they must still be taught how to navigate others safely and critically.
 - 6.14.2. A confidential and accessible helpline would be necessary recognising that children may be reluctant to report prohibited behaviour to adults or may avoid seeking help for fear of punishment or shame.
 - 6.14.3. A ban does not eliminate the need for other support services; in many cases, it may increase demand by complicating where and how children seek help.

¹⁷ <https://www.theguardian.com/australia-news/2025/jul/29/children-to-be-banned-from-having-youtube-accounts-as-albanese-government-backflips-on-exemption>

¹⁸ <https://www.bbc.com/news/articles/cn72yjdj70g5o>

7. Netsafe’s role in helping to change the dial

- 7.1. Netsafe plays, and will continue to play, a critical and unique role in addressing and reducing online harms experienced by children in New Zealand. Drawing on our strengths in education, support services, and systems advocacy, Netsafe will continue efforts to empower tamariki, rangatahi, whānau, and educators with the knowledge, tools, and confidence to navigate online environments safely. We deliver age-appropriate, evidence-based education programmes across schools, kura, and communities, and provide trusted professional development for educators and frontline workers.
- 7.2. Netsafe also operates a free, accessible, and child-friendly support service for online harms, ensuring timely and effective responses for young people and their families. With deep insight into the real-world experiences of children online, Netsafe can use its case data and frontline knowledge to inform policy development, platform accountability, and the design of safer digital spaces.
- 7.3. We also advocate and will continue to ensure that all interventions are responsive to the diverse needs of children, including Māori, Pacific, disabled, and rural young people. Netsafe’s commitment to collaboration means we actively connect government, industry, NGOs, and community groups, while also contributing to international thought leadership in online safety. Through our work, Netsafe aims to drive enduring and equitable improvements in the online experiences and wellbeing of all children in New Zealand.

8. Conclusion

- 8.1. New Zealand should take the time to get this right. That means closely monitoring how similar measures perform overseas, gathering robust evidence through pilots and research, and ensuring any eventual policy response is proportionate, age-appropriate, and grounded in the best interests of children. Technology will continue to evolve but so too must our understanding of how best to support children’s safety, wellbeing, and digital inclusion.

Summary of Key Roles in Reducing Online Harm for Children

Sector	Role
Government	<ul style="list-style-type: none"> • Create and enforce online safety laws (e.g. HDCA, privacy, content standards) • Fund education, prevention, and support services • Lead cross-sector coordination • Fund and share research • Run public awareness/media literacy campaigns
Business	<ul style="list-style-type: none"> • Build in safety-by-design (age-appropriate design, moderation) • Be transparent about policies and impacts • Provide effective user tools (reporting, privacy, parental controls) • Collaborate with NGOs/regulators • Limit children’s data use
Civil Society	<ul style="list-style-type: none"> • Advocate for children’s rights and needs • Deliver school/community education programmes • Provide support (helplines, counselling, legal advice) • Monitor risks and good practice • Empower children/whānau with skills and confidence
Parents & Whānau	<ul style="list-style-type: none"> • Talk regularly with children about online life • Offer support when issues arise • Set boundaries and use safety tools • Build personal digital literacy and role model good behaviour
Schools and Educators	<ul style="list-style-type: none"> • Teach digital citizenship, critical thinking, online ethics • Identify/respond to online harm • Partner with whānau, NGOs, authorities • Include student voice in creating safe spaces
Children and Young People	<ul style="list-style-type: none"> • Contribute to policies and product design • Support peers and call out harm • Seek help when needed • Act respectfully and safely online