New Zealand House of Representatives
Te Whare Māngai o Aotearoa

Education and Workforce Committee
Komiti Whiriwhiri Take Kuranga, Take Hunga Mahi

54th Parliament
March 2026

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

Final report

Presented to the House of Representatives
by Katie Nimon, Chairperson

Contents

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

Summary of recommendations

The Education and Workforce Committee has conducted an inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in addressing those harms, and makes the following recommendations to the Government.

Many of our recommendations received unanimous support. For some recommendations—3, 4, 5, 6, 7, 8, and 12—ACT New Zealand has expressed a differing view or disagree that these are definitive priorities. The Green Party of Aotearoa New Zealand has expressed a differing view related to recommendation 4.

1. **Address legislative gaps and overlaps**
   We recommend that the Government review the legislative framework for online safety, including, but not limited to, the Films, Videos, and Publications Classification Act 1993 and the Harmful Digital Communications Act 2015, to:
   - address current and emerging risks
   - introduce new offences and penalties associated with online harm.
2. **Strengthen liability for online harm**
   We recommend that the Government review the legislative framework for online safety, with a particular view to increasing platforms' civil and regulatory liability for harm resulting from:
   - the content they host
   - platform design (such as use of algorithms and infinite scroll features).
3. **Establish an independent national regulator for online safety**
   - We recommend that the Government establish an independent national regulator for online safety in New Zealand. The regulator should have a full suite of modern regulatory tools and a flexible mandate that allows it to be nimble in response to emerging harms and technologies.
   - We recommend that the Government propose empowering this regulator to make, or advise the Minister on, secondary and tertiary legislation to give effect to regulatory proposals within its intended mandate.
4. **Introduce age restrictions for social media platforms**
   We recommend that the Government progress its consideration of restricting social media access for under-16-year-olds, noting that the majority of us consider doing so is necessary to mitigate the harms young New Zealanders face online.

5. **Ban "nudify" apps and prohibit the creation and distribution of non-consensual deepfake sexual imagery**
   We recommend that the Government take immediate action to condemn and ban all web- and device-based applications that automate or substantially lower the technical barrier to creating deepfake sexual imagery of real people.
6. **Explore options to regulate deepfake technology**
   We recommend that the Government explore options to regulate deepfake technology as part of a wider legislative and regulatory review, or task this to the regulator to prepare further advice on.
7. **Regulate algorithmic recommendation systems**
   - We recommend that the Government closely consider taking action to regulate recommendation systems and take note of the options we have presented for this intervention.
   - We recommend that the House take note that members of the Labour Party of New Zealand would recommend that Government regulate recommendation systems, rather than closely consider taking action.
8. **Mandate algorithm transparency**
   - We recommend that the Government explore:
     - introducing powers for a regulator to require information from platforms relating to their algorithms
     - introducing requirements for platforms to provide accredited researchers with access to information about algorithm design and operation
     - regulating in a manner consistent with the EU or other counterparts.
   - We recommend that the House take note that members of the Labour Party of New Zealand would recommend that the Government undertake the actions described above to mandate algorithm transparency, rather than explore them.
9. **Restrict online advertising of alcohol, tobacco, and gambling**
   We recommend that the Government regulate to prevent online advertising of restricted goods to young people under the age of 18, in a way that aligns with the relevant offline advertising restrictions.
10. **Educate and empower parents, caregivers, and young people**
    We recommend that the Government invest in public online safety campaigns or consider ways to fund the creation and promotion of comprehensive resources designed to educate and inform parents, caregivers, and young people about online safety.
11. **Promote New Zealand-based research**
    We recommend that the Government promote further research grounded in the New Zealand context, further deriving benefit from our recommendation to mandate algorithm transparency.
12. **Consider further matters**
    We recommend that the Government consider each of the matters set out in Chapter 4 of this report and/or task them to the regulator recommended above to further consider, as appropriate.

1 Introduction

This inquiry seeks to examine the harm young New Zealanders encounter online and identify proportionate, actionable interventions to address those harms. It aims to contribute to wider discussion by the Government, members of Parliament, and civil society and gather anecdotal and empirical evidence on online safety in New Zealand.

We conclude that harm to young New Zealanders from online platforms is severe and requires urgent responses from Government, business, and society alike. We consider that online harm needs to be treated as a multifaceted education, public health, and wider governmental issue. We are deeply concerned by the known and potential effects of online harm on youth development and wellbeing. Our overarching conclusion is that the Government should consider ways to improve institutional frameworks, education, and legislation underpinning the regulation of online safety, and take further steps to support parents and caregivers in protecting their young people.

Online harm is fast-moving and occurring on a global scale. One of our key takeaways from this inquiry is that regulating offshore companies' activities within New Zealand is particularly difficult in an online context. New Zealand's economic might is unlikely to be persuasive enough to drive change for offshore companies that provide online services accessible by New Zealand youth.

We therefore consider that New Zealand's best hope to address harms of all kinds from online platforms is to align itself with other countries. In particular, we view the European Union (EU), the United Kingdom (UK), and Australia as countries New Zealand should seek to align itself with. Regulating to prevent online harm is an international movement, often with broad political support, and we strongly consider that New Zealand should be part of it.

We believe New Zealand should be a "fast follower" rather than a "first mover" internationally. That said, it cannot allow itself to be left behind as others take strides to create a safe online environment for young people. In our assessment, we have concluded that lagging behind other countries, or trying to be "unique" in our approach (beyond what is necessary to create supporting domestic infrastructure suited to our laws and context) would both result in poor outcomes for New Zealand's rangatahi (youth).

We presented an interim report on this inquiry in December 2025.[1] It set out the evidence and advice we had received up to then and signalled areas for our further consideration. In this report, we elaborate on our earlier statements, provide further analysis, and make recommendations to the Government.

[1] Interim report on the Inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in addressing those harms | Education and Workforce Committee.

1.1 Our view of how New Zealand should address online harm

Our recommendations are interrelated and rely on these foundational statements, which we believe should underpin New Zealand's next steps:

- Online harm is an issue that requires urgent intervention and should be approached as a public health issue. Online experiences have real-world health implications, mentally, physically, and developmentally. It can also affect school attendance and educational outcomes.
- Regulatory change is necessary to address online harm and clarify the responsibilities that online platforms, parents, and young people each have for this purpose.
- Effective regulatory change cannot be accomplished without an empowered regulator. Most of us consider that this should be a new independent national regulator with a broad and flexible mandate.
- Education is itself a necessary tool to combat online harm, especially for parents and caregivers. Government has the tools to progress national-level education campaigns that could have immediate benefit to parents' empowerment and young people's experiences.

In our terms of reference,[2] we specified that we would assess any recommendations for:

- proportionality, including efficacy, workability, severity, and likelihood of harm
- cost-effectiveness
- intrusiveness and coerciveness
- the speed and practicality of implementation.

Throughout this report, we refer back to these criteria and outline the implications of our recommendations against each criterion.

We have considered other jurisdictions' approaches to addressing online harm. The majority of us consider that the EU's regulatory regime, including its Digital Services Act,[3] is the closest example of how we envisage New Zealand regulation could evolve. In particular, we see it as a model for how platforms could proportionately be held liable for hosting harmful and illegal content, should the Government agree to explore this further. However, we also have a lot to learn from recent experience in Australia and the UK.

1.2 Our desired future state

The majority of us have agreed that the following statements reflect our ideal future state, should the Government agree to implement all our recommendations:

- New Zealand legislation is reviewed and made fit for purpose, enabling a whole-of-system approach to regulating and prosecuting all types of online harm, supported by a national regulator for online safety.

2 See Appendix B or Terms of reference | Education and Workforce Committee.

3 The Digital Services Act | European Commission.

- Social media platforms are required to adopt a safety by design approach to new features and technologies, ensuring the onus is on the platform proving they are safe prior to introduction.
- New harms are quickly identified and responded to, in line with overseas counterparts, because regulatory approaches introduced in New Zealand are sufficiently agile to respond to new developments as they occur.
- Social media use is restricted for under-16-year-olds, with options remaining for youth to engage with appropriately moderated services that are of educational, emotional, social, and civic benefit.
- "Nudify" apps are banned, and other deepfake tools expressly regulated to prevent abuse.
- Online advertising of harmful products, such as alcohol, tobacco, and gambling for under-18-year-olds is effectively regulated and aligned with offline regulations, including for under-18 year olds.
- Online platforms can be held to account when necessary for hosting harmful and illegal content through their services.
- Parents and caregivers feel empowered and informed to play their part in protecting young people from online harm.
- Algorithm transparency is required of all platforms providing online services in New Zealand.
- Further academic and national-level research about online experiences in New Zealand is actively encouraged, and more is starting to be published.

1.3 Purpose of this final report

We see this final report as a step towards the necessary action by Government and the private sector alike. We have prioritised concluding this inquiry in time for the current Government to take our recommendations into consideration and to support public discourse on what we see as generationally defining issues of harm minimisation.

We have made efforts to narrow the field of policy considerations to the interventions we believe would be most effective and could be implemented within a short time frame, if appropriately supported. We also propose system reform that would enable a more effective approach to regulating online safety and provide a framework with greater agility for a national regulator to respond to the next generation of technological advancements.

At the end of this report, we also highlight areas where we believe the Government would be best placed to undertake further comprehensive analysis, while exploring the more tangible and immediately actionable solutions we have identified.

2 The roles of Government, business, and society

2.1 The role of Government

Most of our recommendations in this report are addressed to the Government. However, we are of the view that effective implementation of our recommendations would require social and behavioural change on a much wider scale. Government, businesses (including online platforms and social media companies), and civil society (including parents and young people) will all have to play a part to improve online safety in New Zealand.

2.2 The role of parents

We consider that parents and guardians must play a pivotal role to help keep young people safe online. While we have chosen to focus our recommendations on actions we believe the Government should take, the importance of parental involvement to help ensure young people's safety cannot be overstated. Parents are inherently one of young people's first ports of call for support to stay safe online, or for advice if they encounter online harm. Parents and caregivers can also play an important role in ensuring that any government intervention is effective.

However, we acknowledge the need to enable parents to carry out this responsibility effectively. Parents and guardians themselves need access to appropriate tools and education on online safety to effectively support young people to navigate the online world. We consider that more needs to be done, both by businesses and through government, to enhance all adults' ability to carry out their duty of care to the young people under their guardianship.

We elaborate later in this report on how we envision parents and caregivers could be better empowered and educated to support young people online.

2.3 The role of businesses that operate online platforms

As we stated in our interim report, we do not consider that online platforms are doing enough to address the gravity of the harm experienced by young people online. We acknowledge that companies are continually investing in measures that respond to international calls—from governments, consumers, and researchers alike—for meaningful protections from online harm. However, we are not convinced that these measures are sufficient to address the level of risk experienced by young people online. Similarly, we consider that the pace of these developments is too slow to catch up with new and emerging risks to online safety. We also consider that companies' commercial imperatives create inherent and continual barriers to prioritise user engagement over young users' wellbeing.

We have reached a view that the Government should play a stronger role in regulating online safety, including the design of online platforms and mandating online platform safety features. We include several recommendations in this report that call for regulatory changes

to this effect. The extension of civil and regulatory liability to online platforms should also be seriously explored by the Government.

We hope that the majority of online platforms will appreciate the need to prevent harm to New Zealand's young people and be willing to comply with reasonable requirements. We expect that any new interventions would be consistent with interventions in other jurisdictions, which would reduce the potential complexity and cost to platforms of complying with an enhanced domestic regulatory regime and its enforcement. The more that private businesses are willing to comply with and contribute to international online safety efforts, the greater the positive outcomes can be expected to be.

3 Our recommendations to the Government

In this chapter, we explain our recommendations to the Government to improve online safety for young people in New Zealand. We see our first three recommendations as advocating for a "systems-level" change to improve the national framework we use to regulate online harm. The next nine recommendations are for more specific or targeted interventions. In each section we summarise the advice we received and our analysis related to each topic, assess each recommendation against the criteria we set out in our terms of reference, and state our recommendation.

3.1 Address legislative gaps and overlaps

New Zealand's response to online harm is limited by the fragmented approach in our legislative and institutional frameworks to regulating online safety. Responsibility for online harm response and regulation is spread across multiple agencies and pieces of legislation. This fragmentation creates coordination challenges and inefficiencies. There appear to be both gaps and overlaps at various points in what different entities are responsible for and have the power to do. Certain types of harm are subject to overlapping responsibilities from multiple agencies. Other types of harm, particularly those arising from platform design features or emerging technologies, do not clearly fall under any agency's mandate or powers to respond.

Current legislation is not fit for purpose

The majority of us consider that the approach to regulation in the Films, Videos, and Publications Classification Act 1993 and the Harmful Digital Communications Act 2015 is not fit for effectively regulating the online environment. The current approach under the Films, Videos, and Publications Classification Act enables individual pieces of content to be classified and restricted or made illegal, depending on the level of harm. This framework is necessary to responding to instances of extreme harm. However, the majority of us believe there could be benefit in taking a proactive, system-wide approach to social media and other online platforms that incorporates reactive and proactive regulatory levers.

We consider that the current legislation does not set appropriate offences and penalties for the types of harm that have been shared with us. We believe that the harm caused to New Zealand's young people through a variety of online platforms warrants a comprehensive liability regime that sets regulatory offences and penalties, as well as opening online platforms to private and class action through pecuniary penalties.

In addition, we note that the current framework is not always enforceable. In particular, we would like to see the Government take steps to ensure that online platforms can be held liable for harm experienced through the platforms they host or operate.

Summary of our analysis: Addressing legislative gaps

Criteria	Our assessment
Proportionality	We have identified gaps in the legislative framework that we consider need to be addressed with some urgency. We encourage the Government to consider whether the gaps are wider than we understand them to be, in which case a more comprehensive review may be even more desirable.
Cost-effectiveness	The act of reviewing legislation can be resource intensive, but this would likely be manageable within departmental baseline, notwithstanding the potential need to reprioritise other work with the Government's agreement. We expect that any proposal to the contrary would require ministerial and Cabinet authorisation.
Intrusiveness	We expect that the Ministry of Justice, the Ministry for Regulation, and the Office of the Privacy Commissioner would be among those consulted on these matters in the normal course of Government policy development.
Speed of implementation	A first-principles review will be needed at some point but could take several years to scope and test before the Government could draft proposals. Based on our criteria for this inquiry, we recommend first that the Government prioritises addressing complete gaps in the legislation and reviews the liability provisions that online platforms can be subject to.

Recommendation

1. **Address legislative gaps and overlaps**
   We recommend that the Government review the legislative framework for online safety, including, but not limited to, the Films, Videos, and Publications Classification Act 1993 and the Harmful Digital Communications Act 2015, to:
   - address current and emerging risks
   - introduce new offences and penalties associated with online harm.

3.2 Strengthen liability for online harm

There are existing liability provisions in New Zealand law related to objectionable content under the Films, Videos, and Publications Classification Act.[4] There are also provisions in the Harmful Digital Communications Act that place the onus on platforms to respond to complaints.[5] However, there are no legal requirements in New Zealand for platforms to proactively implement safety measures to keep children safe from online harm. There are also no legal requirements in New Zealand for platforms to support parents in keeping their children safe on online platforms.

[4] Content is considered objectionable if it describes, depicts, expresses, or deal with matters such as sex, horror, crime, cruelty, or violence in such a way that it is likely to be harmful to the public good. Objectionable content is illegal.

[5] Second Departmental Report | Departmental of Internal Affairs, pp 15–17.

We consider this does not reflect the gravity of online harm and that, in the longer term, a first-principles review of the online safety regulatory system would be beneficial. However, such reviews take time, while harm is occurring right now. Because of this, we also make recommendations in this chapter for actions that could be prioritised so that some change can be actioned with the urgency this problem requires.

The balance of protections and obligations on platforms is not right

We note that the term "online platforms" spans a wider range of businesses than "social media"—we discuss the latter later in this report.

We consider that there may be serious gaps in the current framework:

- Instead of incentivising proactive prevention of harm, the law rewards companies for responding "positively" to harm experienced by users on their platforms, which in our view they should be held at least partly liable for.
- There are no obligations on platforms to proactively identify or prevent harmful conduct.
- There is currently no equivalent framework for holding platforms accountable for harmful design features or internal systems that enable the proliferation of legal-but-harmful content.

Protections for online platforms from liability may not serve the public interest

New Zealand law includes protections from liability for platforms, in the form of "safe harbour" provisions, including under the Harmful Digital Communications Act. If online platforms follow the "safe harbour" process, they cannot be held liable for content that other people post on their platforms. The purpose of these provisions is to protect online platforms from being taken to court for content hosted on their service, if they are not aware of the harmful content. Online platforms can be liable if they are notified by a complainant that the content breaches the law and if they do not remove it within 48 hours. However, this means that they also escape most liability for wider social harms resulting from the aggregate of all that user-generated content they host, as long as they continue to react appropriately after individual pieces of content are posted. Notification of harmful content can be generated by a platform's users reporting content. In such instances, harm may already have occurred by the time the platform takes action in response.

The majority of us consider that the safe harbour provisions should be removed, or substantively amended to better reflect the role that online platforms play, whether knowingly or unknowingly, in making harmful content available to users. We note that comprehensive regulatory frameworks often provide a degree of protection to increase compliance and improve regulatory and enforcement outcomes, but we question whether a blanket protection from liability truly serves the public interest in this case. We do not suggest that online platforms should be solely, or even primarily, liable for user-generated content. However, we do not consider that the current balance of legal protections and regulatory obligations on these platforms is correct.

Despite our firm view that safe harbours need to be further scrutinised and tested against the public interest, we also consider that any new liability under New Zealand law should be equivalent to liability in other jurisdictions. We encourage the Government to further explore introducing both strict and limited liability provisions. We understand that New Zealand does

not have international trade obligations that would prevent it from imposing new liability obligations on platforms.

Online platforms should be responsible for age-appropriate online experiences

There is currently no legal framework in New Zealand for holding platforms accountable for harmful design features or content that is not considered objectionable, but may still cause some harm. From the evidence we received, we saw that a significant portion of the harm young people experience does not directly relate to illegal content or behaviours.

Harm can result from exposure to restricted products, such as pornographic services, alcoholic beverages, and gambling sites. Some harm may relate to entirely unrestricted activities, such as varying degrees of extreme weight loss or other body-image related content. Other harms result from platform design features, such as the endless scrolling features that have become prolific on many short-form video platforms.

We do not necessarily consider that these harms and harmful design features could, or should, be made illegal. However, we strongly recommend that online platforms be tasked with a duty of care to young people that extends beyond whether an individual piece of content can be defined as “objectionable” or distressing on its own. We are also concerned that otherwise legal or harmless content can become harmful through prolonged exposure, or by being targeted at a younger audience than appropriate.

We elaborate later in this report on some specific regulatory design proposals related to this issue.

The European Union provides a promising framework to address this

In our view, it would be appropriate to follow the example of the EU and its Digital Services Act and introduce comprehensive, graduated liability for online platforms. Our view is that online platforms should be subject to a mix of preventive obligations (such as duties to design safely) and civil liability (such as responsibility for harm caused).

Under the EU’s Digital Services Act, online platforms are required to proactively take measures to meet their compliance obligations and may face fines of up to six percent of their global turnover. We consider this preventive approach much more likely to address the underlying causes of online harm than New Zealand’s current reactive approach, whereby online platforms are only required to take measures in response to a complaint or take-down notice.

Recommendation

2. **Strengthen liability for online harm**
   We recommend that the Government review the legislative framework for online safety, with a particular view to increasing platforms’ civil and regulatory liability for harm resulting from:
   - the content they host
   - platform design (such as use of algorithms and infinite scroll features).

3.3 Establish an independent national regulator for online safety

There is no single regulator for online harm in New Zealand. We consider that this limits stewardship, strategic vision, and operational efficiency to improve online safety. The topics in this report cover a wide range of regulatory issues that span multiple government agencies and regulatory frameworks. We touched on this complexity in our interim report and have further considered whether this itself is inherently a problem.

Responsibilities to address online harm are instead spread across multiple entities.[6] There are no centralised response, safeguards, or framework—aside from the provision of public information—applicable to the most pressing risks affecting young people. We commend the efforts of all public and private sector bodies that operate in this space, and that work to protect young New Zealanders from harm. However, we think they would be more appropriately supported to face contemporary challenges if the regulation associated with online harm was delivered by a single modern, agile regulator.

We have considered several approaches to achieve this. Some of us consider that existing institutions should be strengthened to fill gaps in the current framework. However, the majority of us consider that the existing framework as a whole is not fit for purpose and that a national independent regulator could better respond to modern and quickly evolving challenges.

Clarifying regulatory arrangements is a precursor to effectively implementing our other recommendations

Many of the recommendations we make in this report depend on there being a clear, well resourced, technologically capable regulator tasked with overseeing their effective and proportionate implementation. Ideally, this would be an entity monitored by a responsible department, or an independent function hosted by a department, rather than a new government department itself. If a standalone entity were to be created, we consider that it would need to have all the following features:

- appropriate powers and resources to implement and enforce the regulatory regime
- clear institutional responsibility for emerging harms that currently fall between existing agencies
- specialist expertise in online safety that can be applied across different types of harm
- capability to assess platform compliance with technical standards
- sufficient resource to monitor platform compliance and take enforcement action where necessary
- the mandate to serve as a single point of contact for the public to report harm and seek assistance, and coordinate with other agencies where required
- coordination mechanisms to ensure agencies work together effectively on harms that cross over their respective areas of responsibility

[6] Entities that have functions related to addressing online harm include the Department of Internal Affairs, the Classification Office, the New Zealand Police, the New Zealand Customs Service, Netsafe, the District Courts, the Advertising Standards Authority, the Commerce Commission, and the Financial Markets Authority.

- a consistent approach to engaging with online platforms
- capacity to represent New Zealand in international forums.

We acknowledge that an alternative approach would be to enhance the powers, functions, and duties of (and potentially funding for) existing agencies, or one particular agency. However, many of us are concerned that this option would not offer the same degree of centralised coordination, regulation, and enforcement of online harm. This approach could retain the existing complexity and inefficiencies in the system today, and increase the future risk that online safety resources could be directed towards other policy objectives of the day.

New Zealand can learn from other jurisdictions

Other jurisdictions, such as the UK, Ireland, and Australia, all have national online safety regulators. For example, the UK's Online Safety Act 2023 empowered Ofcom as an independent regulator to enforce and monitor legal requirements on online platforms to protect children and young people from harm.[7] Ireland's Online Safety Commissioner issues an online safety code to set out actions that online platforms must take to protect the public from harmful content.[8]

The Australian eSafety Commissioner has a range of powers and responsibilities, including:

- the ability to issue notices to require online services, internet search engines, and internet service providers to take measures to remove illegal content, or access and links to illegal material
- the ability to require platforms to report on their compliance with Australia's Basic Online Safety Expectations[9]
- advising educators, parents, and young people on online safety
- conducting research related to online safety.[10]

We consider that lessons could be learned and certain design features could be borrowed from those jurisdictions.

Designing a regulatory regime for online safety

Consistency with the Government's expectations for good regulatory practice

We consider that establishing a clear regulatory framework to address online harms, create clear legal liabilities, and mandate protections for young people would improve online safety in New Zealand. A national regulator could oversee the implementation of such a framework. We believe that online safety regulation would align prevention of online harm with the Government's expectations for good regulatory practice.[11] In particular, we hope to see intentional shifts to ensure that this regulatory regime:

- has clear objectives, as well as clear division of responsibilities between agencies
- achieves its objectives in a proportionate and cost-effective manner

7 Ofcom.

8 Ireland's media regulator | Coimisiún na Meán.

9 Basic Online Safety Expectations | eSafety Commissioner.

10 What we do | eSafety Commissioner.

11 Government Expectations for Good Regulatory Practice | New Zealand Government.

- is nimble and resourced to allow the appropriate regulator to adapt their regulatory approach to different regulated parties, and to encourage innovation in efficient and safe approaches to meeting their regulatory obligations
- is an active participant and fast follower in international discussions and overseas initiatives to address online harm
- minimises unintended gaps or overlaps and inconsistent or duplicative requirements
- sets out legal obligations and regulator expectations and practices in ways that are easy to find, easy to navigate, and clear and easy to understand
- has scope to evolve in response to changing circumstances or new information on the regulatory system's performance and new technologies.

Regulating the online environment creates unique challenges. Key considerations for regulating in the digital age include the following:

- **Safeguards to protect rights and freedoms**—Appropriate safeguards would be essential to ensure a regulator with broad powers does not impose excessive compliance burdens on platforms or make decisions that unduly restrict freedom of expression. International experience suggests that finding the right balance between protecting users and avoiding overreach is challenging. Clear statutory limits on powers, review mechanisms, and transparency requirements would be important design features.
- **Coordination with existing agencies and legislation**—Establishing a new regulator presents an opportunity to resolve coordination problems, but achieving this in practice would require careful design of the institutional framework. A new regulator would need to either establish clear working relationships with existing agencies or absorb those agencies, and relationships with existing legislation would need to be clearly articulated.
- **Crown funding implications**—Adequate resourcing is essential for regulators to fulfil their functions effectively. It is not clear from our initial consideration that cost recovery would be feasible for the services that would be provided by this proposed public good regulator. Every action and intervention would require some degree of ongoing resourcing, including education and public awareness activities. Currently, online safety resources are concentrated on criminal investigations and the most high-risk cases, with cases heavily triaged and prioritised. Other parts of the system require people affected by online harm to take action themselves, for example by changing their account settings or collecting evidence of harms they experience themselves. This requires considerable effort on the part of potential victims.
- **Enforcement limitations**—As indicated earlier, we consider that New Zealand should not attempt to overcome online safety concerns alone on the global stage. While a single regulator would be likely to enhance New Zealand's ability to establish effective relationships with overseas-based platforms, enforcement against platforms headquartered overseas presents ongoing challenges. New Zealand can take different approaches to platforms that are willing to be regulated and those that are not. Compliance and enforcement are likely to improve over time in collaboration with other countries' efforts.

Consider hosting a regulator within an existing agency as an interim step

Our preference is for a new independent national regulator to be established. We acknowledge that it would take both time and resources to set up a new regulator. Nonetheless, we see this as an urgent change that needs to be prioritised. We would encourage the Government to consider proceeding by first establishing a new regulator within an existing agency as soon as possible. This could enable the Government to test this approach and allow the new regulator to grow quickly, drawing from existing relationships and expertise.

This could look similar to the Charter School Agency within the Ministry of Education, or the establishment of Invest New Zealand, initially hosted within New Zealand Trade and Enterprise, which is now in the process of becoming a standalone agency with its own board; both agencies are effectively pursuing the Government's agenda.

Summary of our analysis: Establishing an independent national regulator for online safety

Criteria	Our assessment
Proportionality	We consider this to be the single most effective recommendation we make from a system stewardship, implementation, and enforcement perspective. It would also provide a foundation for other regulatory interventions.
Cost-effectiveness	We have not specifically sought to model the costs associated with this option, but acknowledge that this is likely to be our most costly recommendation. Most of us believe the cost would be proportionate to the scale of the harm it would address. We also consider that it would not be feasible to address online harm without incurring cost, and we would expect a single, focused regulator to provide the most efficiency for this investment in the long run.
Intrusiveness	Establishing a national regulator has the potential to be intrusive, depending on what powers and functions it is tasked with. An appropriate balance between intrusiveness and risks should be considered in the design of legislation establishing the regulator.
Speed of implementation	It could take up to 2–3 years to establish a new, independent regulator. We expect this could begin sooner if the regulator was initially established within an existing agency.
Comment	The majority of us contend that there is a strong case that having a singular regulator would better enable young people and their parents and caregivers to seek support and know where to go for information on online harm. If New Zealand introduced a national regulator for online safety, the majority of us are strongly of the view that it should be empowered to be sufficiently agile to address the development of new technologies and platforms as they arise.

Recommendation

3. Establish an independent national regulator for online safety

- We recommend that the Government establish an independent national regulator for online safety in New Zealand. The regulator should have a full suite of modern regulatory tools and a flexible mandate that allows it to be nimble in response to emerging harms and technologies.
- We recommend that the Government propose empowering this regulator to make, or advise the Minister on, secondary and tertiary legislation to give effect to regulatory proposals within its intended mandate.

3.4 Introduce age restrictions for social media platforms

The Minister of Education is leading a Government work programme to explore options to restrict young people under the age of 16 from accessing social media.[12] The Prime Minister has stated his intention to introduce legislation before the end of 2026. Catherine Wedd MP has also put forward a member's bill that would restrict access to social media platforms for under-16-year-olds. The bill was introduced to Parliament in October 2025.[13]

We have not undertaken a detailed analysis of the costs and benefits of this proposal, as the Government will have far greater access to the relevant information than we do. However, most of us strongly support the proposal to restrict access to social media for under-16-year-olds. We note that many submitters said that establishing an age limit for social media would help to signal expectations about appropriate social media use for parents, carers, and young people. Submitters suggested that New Zealand learn from, and potentially model its approach on, age-based restrictions recently introduced in Australia.[14] We understand that other jurisdictions have also recently announced their intentions to explore restricting access to social media for under-16-year-olds, including the UK in January 2026,[15] and Spain in February 2026.[16]

Design concerns associated with age restrictions on social media

Several barriers to effective implementation of age restrictions would need to be considered in designing New Zealand's approach:

- **Privacy risks**—Some submitters highlighted the potential privacy risk of requiring age verification, as it would likely involve sharing proof of identity which could increase the risk of identity theft.
- **Ease of evading restrictions**—We acknowledge that attempts to control online activity can be evaded by using Virtual Private Networks (VPNs) to suggest that a person is in a different jurisdiction. We have not identified a solution to this limitation, but refer to it later as an area that warrants further exploration by the government. We note that age-

[12] Minister to lead work on reducing social media harm for under-16s | Beehive.

[13] Social Media (Age-Restricted Users) Bill 216—1 (2025), Members Bill | New Zealand Legislation.

[14] Online Safety Amendment (Social Media Minimum Age) Act 2024 | Federal Register of Legislation.

[15] UK to consult on social media ban for under 16s | BBC.

[16] Spain announces plans to ban social media for under-16s | BBC.

based restrictions may not work in isolation, and that other complementary measures may need to be explored.

- **Inconsistent requirements across different types of online platform**—One of the most technically difficult elements we foresee for drafting legislation to restrict social media access is how to define social media itself. We provided one definition in our interim report, but a number of academically accepted definitions exist.[17] In other jurisdictions, age restrictions have failed to be applied to all platforms where peer-to-peer interaction happens and harm occurs. Restrictions have also been applied to some educational platforms, or platforms where a lesser degree of harm occurs.
- **Undermining benefits of online technologies**—Age restrictions in other jurisdictions have been applied to some educational platforms or platforms where less harm occurs. As set out in our interim report, we acknowledge the many benefits that social media can have for positive interaction and access to educational resources. We do not want our recommendation to be implemented as a ban on appropriately moderated forums. These can serve as a useful tool for positive social interaction, access to support networks and services, youth civic participation, or educational advancement.

The Office of the Privacy Commissioner, among other submitters, spoke to us about the current limitations of age-verification methods. We encourage the Government to consider whether age verification could be approached in a manner similar to identity-verification requirements under New Zealand's anti-money-laundering laws, or using emerging products that are designed to verify age without collecting other identity information.

We consider that the best approach to working through these limitations, where no equivalent regime exists in New Zealand, would be for the Government to work with Australian counterparts. There may be many benefits from learning how the Australian Government approached the design of provisions in the Online Safety Amendment (Social Media Minimum Age) Act 2024. Similarly, it would be advantageous to know whether any unforeseen challenges have arisen since the age restrictions came into effect in Australia in December 2025, and for an appropriate regulator to monitor international experience and evidence over time.

Summary of our analysis: Age restrictions for social media platforms

Criteria	Our assessment
Proportionality	The majority of us consider that this intervention is proportionate to the serious nature of the harm it would mitigate.
Cost-effectiveness	We do not have information on the Government's proposed approach and so have been unable to indicate the cost-effectiveness and financial implications of this intervention.
Intrusiveness	This intervention is highly intrusive compared to the current absence of restrictions. However, most of us believe that the nature of the harms we

[17] In our interim report, we stated: "For the purposes of our inquiry, we use "social media" as an umbrella term encompassing websites and applications that allow users to create, share, and view digital media and communicate with each other. For example, social media platforms include, but are not limited to, Facebook, Instagram, Snapchat, TikTok, and X". Interim report | Education and Workforce Committee, p 8.

Criteria	Our assessment
	have heard about—through evidence, anecdote, lived experience, and advice—warrants such intrusion.
Speed of implementation	Depending on the Government's approach, we believe this could be implemented very quickly and would hope to see this in effect within the next 12 months.
Comment	Most of us strongly support this intervention and wish to see it implemented as soon as practicable. We urge the Government to commit to this as the most useful immediate solution to prevent further harm.

Recommendation

4. **Introduce age restrictions for social media platforms**
   We recommend that the Government progress its consideration of restricting social media access for under-16-year-olds, noting that the majority of us consider doing so is necessary to mitigate the harms young New Zealanders face online.

3.5 Ban "nudify" apps

The most common method for creating non-consensual sexual deepfakes is through "nudify" apps. These are mobile or web-based applications that enable the creation of false or altered images of real people in a pornographic or highly sexualised manner. There are also various other generative AI tools that enable the creation of non-consensual sexual imagery. While some "nudify" apps include prompts to ask if the user has permission to use someone's likeness before the deepfake is created, we do not consider this an acceptable threshold to check whether meaningful consent has been obtained.

In New Zealand, sexualised images (including deepfake images) of children and young people are considered "objectionable" under the Films, Videos, and Publications Classification Act. For some types of content, a classification of objectionable depends on whether the content describes, depicts, expresses, or otherwise deals with sex in a way that is likely to be "injurious to the public good". The creation of objectionable content carries the most severe penalties under the Act, even if the content is created using an AI tool. In certain circumstances, creation and distribution of deepfakes could also be covered by existing provisions in the Crimes Act 1961. However, there is currently no regulation of deepfake tools or "nudify" apps themselves.

Non-consensual sexually explicit images used as harmful digital communications can also be in violation of the Harmful Digital Communications Act. However, AI-generated images are not specifically covered in that Act and the creation of non-consensual deepfake content itself is not explicitly prohibited.

We are pleased that existing laws have been flexible enough to react to the most harmful conduct through these apps, which meets existing prosecutorial thresholds. We consider it necessary to further regulate deepfake technologies and "nudify" apps that enable the

creation of deepfake sexual imagery of real children, young people, and adults. Overall, we do not think that "nudify" apps should have a role in New Zealand society, and support them being banned.

We urge the Government to ban "nudify" apps with immediate effect

New Zealand would not be the first to take steps to ban such apps, and we do not believe that implementing an initial change would be difficult. The UK Government announced its intent to ban these apps in December 2025. In January 2026, a letter from UK MP Rt Hon Liz Kendall to the UK Parliament's Science, Innovation and Technology Select Committee detailed the UK Government's plans to ban "nudify" apps through the Crime and Policing Bill going through its Parliament now.[18] Australia has also announced that it intends to ban "nudify" apps.[19]

We urge the New Zealand Government to take a similar approach. We note that Laura McClure MP has put forward a member's bill proposing to criminalise the creation, possession, publication, and sale of sexually explicit deepfakes. The bill was introduced to the House in October 2025.[20]

We consider that web- and device-based applications that automate or substantially lower the technical barrier to creating deepfake sexual imagery of real people should be banned. We understand that some technology that enables the creation of deepfake sexual imagery can also be used to create other types of deepfakes for lawful purposes. The intention of our recommendation is to target, regulate, and restrict the use of deepfake tools to prevent sexual abuse. We are most concerned to address the creation and distribution of deepfake sexual imagery of children and young people—something that we consider an extreme harm. Further consideration is needed to appropriately design a ban that would capture applications that enable deepfake sexual abuse and imagery, without unintentionally capturing other technologies and compliant applications. The Government may wish to consider how other jurisdictions, such as Australia and the UK, design and implement such bans.

Summary of our analysis: Banning "nudify" apps

Criteria	Our assessment
Proportionality	We consider that there is no benefit to allowing products on the New Zealand market that have the express intent of creating sexualised images of real people without their consent. Removing these apps directly removes a source of harm.
Cost-effectiveness	We expect this proposal to be low cost in the first instance, as products with this sole purpose are easy to identify and remove or geo-restrict so they cannot be accessed within New Zealand.
Intrusiveness	We consider that it is not "intrusive" to prevent expressly objectionable material in the form of sexualised images of real persons from being created

[18] Letter to Science, Innovation and Technology Committee | Rt Hon Liz Kendall.

[19] Taking a stand against abusive technology | Ministers for the Department of Infrastructure.

[20] Deepfake Digital Harm and Exploitation Bill | New Zealand Legislation.

Criteria	Our assessment
	without their consent. For example, sexualised images of children are already illegal under the Films, Videos, and Publications Classification Act 1993.
Speed of implementation	We hope to see this action taken through the first legislative vehicle available to do this.
Comment	An appropriate interim regulator would need to be nominated to give effect to this recommendation if it can be given effect to prior to a new regulatory structure being implemented.

Recommendation

5. Ban "nudify" apps and prohibit the creation and distribution of non-consensual deepfake sexual imagery
We recommend that the Government take immediate action to condemn and ban all web- and device-based applications that automate or substantially lower the technical barrier to creating deepfake sexual imagery of real people.

3.6 Explore options to regulate deepfake technology

We consider that deepfake technology and other AI-generated imagery needs to be regulated. We agree with submitters who suggested that AI-generated content and deepfakes should be addressed directly in New Zealand legislation. We see this as a legislative gap resulting from the rapid emergence and proliferation of new technologies. We recommend, at a minimum, that the Harmful Digital Communications Act be amended and clarified to expressly address the use of deepfakes and AI-generated content to harm another person.

Recent concerns have emerged in particular regarding the use of Grok, an AI tool available on X, to generate sexual imagery of women and children without consent. In January 2026, X announced that it would geo-block the ability to "generate images of real people in bikinis, underwear, and similar attire" on Grok in locations in which such content is illegal.[21]

We understand that the European Commission and the UK Information Commissioner have both launched investigations into the use of Grok to produce harmful sexual content.[22]

We recommend that the Government act now to ensure that New Zealand is among the countries where features of this kind are removed by design. It may be that current laws are suited for this purpose, but we seek further assurance whether that is the case.

Regulation would send a clear signal that New Zealand is open to beneficial uses of AI-generated content, but does not accept tools being developed without regard to the very real

[21] Geo-blocking refers to restricting access to certain online content in a particular geographical location. Grok Account Image Generation Updates | X.

[22] Commission investigates Grok and X's recommender systems under the Digital Services Act | European Commission ; ICO announces investigation into Grok | Information Commissioner's Office.

harm they could cause. We see a need for clear expectations, and consequences for companies that do not meet them, be that a fine, court action, or removal of services from the New Zealand market.

Regulating deepfake technologies and banning "nudify" apps would require a flexible regulatory approach to respond to the evolution of these technologies and set appropriate safeguards and expectations over time. We consider that a national regulator would be best placed to monitor evolving technologies in this space.

Summary of our analysis: Regulation of deepfake technology

Criteria	Our assessment
Proportionality	We consider it appropriate to regulate the design and use of technologies when the purpose and scope of the regulation is limited to preventing identifiable and foreseeable harm and making it harder for users to create and distribute illegal content.
Cost-effectiveness	Regulation of deepfake technology would be relatively cost effective, as long as was overseen by an appropriate regulator that was enabled to evolve its approach over time.
Intrusiveness	We consider this proposal more intrusive than the proposal to ban "nudify" apps because there are many legitimate uses for deepfake technologies. We are mainly opposed to harmful-by-design or neglectful functionality. The degree of intrusiveness and how easy compliance is for businesses depends on the regulatory approach taken.
Speed of implementation	We think this could be done quickly but suggest it may be more appropriate to build into the design of a new regulator.
Comment	We encourage the Government to progress this proposal as a component of the wider legislative and regulatory reviews we recommend.

Recommendation

6. **Explore options to regulate deepfake technology**
   We recommend that the Government explore options to regulate deepfake technology as part of a wider legislative and regulatory review, or task this to the regulator to prepare further advice on.

3.7 Regulate algorithmic recommendation systems

Many online platforms, such as social media, use recommendation systems to promote content to their users. Recommendation systems use algorithms that sort and prioritise the content that is shown to users. Most recommendation systems are designed to prioritise feeding users content and advertising that is popular or that is similar to what they, or similar users, have engaged with previously. Recommendation systems are used to increase user engagement, based on the assumption that users are likely to use platforms more often and

for longer if the content they see is personalised and interesting to them. User engagement is important to the success of a social media platform's business interests because it correlates with revenue. However, recommendation systems can also amplify content that may increase exposure to, or exacerbate, online harms.

We have considered several options for regulating recommendation systems. The first, and arguably most obvious, option would be to prohibit the use of recommendation systems on young people's accounts. Recommendation systems could alternatively be regulated by requiring platforms to adjust algorithms to hide or deprioritise harmful content or provide easy-to-access ways for users to opt out of these systems. A less intrusive option would be to strengthen algorithm transparency and require online platforms to proactively inform users about how they can have more control over what they see on social media. We elaborate on this option later in this report.

Our view is that these could all be viable options in the New Zealand context. However, this is one area where international debate is ongoing and it would be prudent for the Government to explore options further and learn from overseas counterparts.

In particular, this is one area where we consider that aligning with the United States would lead to the greatest ease of implementation. Many of the most prevalent online platforms are headquartered in the USA, and others may be more likely to comply with US requirements given the size of its population and the market it offers. Two bills are currently before the US Senate that we are watching with particular interest:

- S.278 - Kids Off Social Media Act—a bill that, if enacted, would prohibit social media companies from "using automated systems to promote content based on personal data for people under the age of 17".[23]
- S.1748 - Kids Online Safety Act—a bill that proposes to allow children and young people to opt out of recommendation systems, strengthen default privacy settings, and enable stronger parental controls. This proposal is currently being considered by the US Senate's Commerce, Science, and Transportation Committee.[24]

We note that the efficacy of regulation like that being considered by the Senate may not be an efficient intervention here if progressed alongside restrictions on under-16-year-olds using social media. However, it may still be effective as a signal (or set of requirements) for any platforms that were not subject to such a restriction.

We consider that there would be benefit to considering whether young people over the age of 16 would be best protected by provisions similar to those in the US Kids off Social Media Act. The ability to opt out of recommendation systems or use strengthened parental controls could also be applied to social media accounts for young people aged between 16 and 18 years old.

We understand that the Spanish Government has recently announced its intention to make it a criminal offence to manipulate algorithms on online platforms to amplify illegal content.[25]

---

[23] Senate Report, Kids Off Social Media Act | Library of Congress.

[24] Kids Online Safety Act | Library of Congress.

[25] Spain announces plans to ban social media for under-16s | BBC.

Summary of our analysis: Regulating recommendation systems

Criteria	Our assessment
Proportionality	We consider that requiring online platforms to proactively inform users about how they can have more control over what they see on social media, and educate parents on the tools available to them, would be a bare minimum regulatory intervention. We consider the other options we have considered are proportionate to the harm, but less workable if not done in a manner consistent with other jurisdictions.
Cost-effectiveness	The cost of compliance for businesses, and of enforcement for Government, is hard to determine without further analysis and selecting a specific intervention.
Intrusiveness	Regulating recommendation systems would be intrusive on affected businesses, potentially including their intellectual property. Our assessment is that implementation by social media companies would be relatively straightforward, minimally intrusive, and easy to comply with, if it matched any future requirements set in US law. Few online platforms that operate in New Zealand, and would likely be affected by this change, do not also operate in the USA.
Speed of implementation	Any kind of regulation of recommendation systems is likely to require legislative change. It could be progressed in tandem with other proposals we recommend.
Comment	We consider that this recommendation would be less necessary as an intervention to online harm faced by young New Zealanders if the Government progressed its intent to restrict social media access for under-16s. We make a further recommendation on regulating for algorithm design and transparency below.

Recommendation

7. Regulate algorithmic recommendation systems

- We recommend that the Government closely consider taking action to regulate recommendation systems and take note of the options we have presented for this intervention.
- We recommend that the House take note that members of the Labour Party of New Zealand would recommend that Government regulate recommendation systems, rather than closely consider taking action.

3.8 Mandate algorithm transparency

We consider that there is strong public interest in information on platform's algorithm design being made available, especially for regulatory and research purposes. We acknowledge that there are technological complexities and commercial sensitivities involved in algorithmic design which would need to be accounted for in designing regulations. We do not expect

New Zealand to develop unique requirements in this area. Rather, we consider there are good opportunities to implement approaches already used in other jurisdictions.

We suggest considering requirements to improve algorithm transparency that are consistent with the EU's approach. New Zealand could introduce similar requirements for platforms to provide researchers with access to information on algorithm design and operations. We understand that the Australian eSafety Commissioner is empowered to require online services to provide information about how their use of algorithms may contribute to or reduce the risk of online harm. If an online regulator is established in New Zealand, it should also be empowered to require information from online platforms related to algorithm design and operation.

This proposal would be supplementary to wider regulatory reform and does not replace the need for greater regulation.

Summary of our analysis: Regulating algorithm design transparency

Criteria	Our assessment
Proportionality	This proposal would support regulatory oversight and create incentives for platform behaviour change. It is aligned with international moves to require algorithm design transparency.
Cost-effectiveness	Highly cost-effective if New Zealand requirements do not exceed international requirements. Likely to drive behaviour change from companies and improve regulatory oversight and research data.
Intrusiveness	We consider that intrusion on commercially sensitive information is justified by the public interest in transparency. Also, concerns of intrusiveness in this instance are somewhat mitigated by existing requirements to provide this same information in other comparable jurisdictions.
Speed of implementation	This would be relatively quick to implement, subject to the availability of a legislative vehicle for the change.
Comment	Due to the inherent technical complexity in this proposal, we recommend that New Zealand mirror another jurisdiction's approach, to enhance workability and the likelihood of compliance with new requirements.

Recommendation

8. Mandate algorithm transparency

- We recommend that the Government explore:
  - introducing powers for a regulator to require information from platforms relating to their algorithms
  - introducing requirements for platforms to provide accredited researchers with access to information about algorithm design and operation
  - regulating in a manner consistent with the EU or other counterparts.

- We recommend that the House take note that members of the Labour Party of New Zealand would recommend that the Government undertake the actions described above to mandate algorithm transparency, rather than explore them.

3.9 Restrict online advertising of alcohol, tobacco, and gambling

Restricting online advertising of harmful products would be likely to address harm by reducing young people's exposure to persuasive marketing, helping to limit the normalisation of alcohol, tobacco, and gambling, and reducing early initiation and associated harms.

Under existing laws, advertising that has special appeal to young people or promotes excessive consumption can already be prohibited, such as tobacco and vaping under the Smokefree Environments and Regulated Products Act 1990. We consider that there are compelling social and health reasons to extend this to other restricted goods, and take a more proactive approach to ensuring that restrictions on advertising are being applied consistently across restricted products and online platforms.

We consider enforcement to be an important element of this proposal. We do not believe it is right for proactively compliant companies to be commercially disadvantaged because other platforms or businesses are unwilling to comply and continue to derive revenue from potentially harmful advertising.

We understand that in October 2025, the Petitions Committee recommended that the Government review the regulatory settings around gambling advertising in New Zealand.[26]

Implementation requirements

The design of this intervention would need to take account of the following concerns:

- **A responsive regulatory approach**—Monitoring and enforcing large volumes of digital content across platforms could require significant resources, especially if the restriction is only on advertising aimed at young people. We therefore consider that this matter would be most appropriately tasked to a national regulator whose resources could be directed to the areas of greatest harm and non-compliance over time.
- **Technical complexity of online advertising**—We acknowledge that defining and regulating online advertising (especially influencer marketing and algorithmic delivery) is technically complex. Platforms may need new age-verification and content classification systems, and these platforms may be additional to those captured by our other recommendations.
- **Commercial implications of limiting advertising**—While the Government may wish to consider whether these products should be restricted in advertising more generally, as is already the case for smoking and vaping products, that is beyond the scope of our inquiry. The intent of our recommendation is that it would only apply to under-18-year-

[26] Petition of Problem Gambling Foundation of New Zealand: Prohibit the advertising of gambling | Petitions Committee.

olds. A wider application of our recommendation would limit what is currently legitimate adult advertising and a source of revenue for online platforms.

Effective restrictions would require consistent application across platforms, strong age-targeting controls, and ongoing monitoring mechanisms. A regulator tasked with overseeing these restrictions would need a suite of regulatory tools to respond proportionately to companies that are willing to comply and those that are not willing or do not know how to comply. The regulator would also need adequate resourcing for implementation, monitoring, and enforcement.

We recommend that the Government consider whether it would be more efficient to build on the existing frameworks to regulate advertising, or whether this matter should be tasked to a new regulator as part of the wider response to online harm.

Summary of our analysis: Restrictions on the online advertising of alcohol, tobacco and gambling

Criteria	Our assessment
Proportionality	Effective implementation would prevent early exposure to addictive, restricted goods through online channels. Young people would still be exposed to peer pressure or adult social norms offline, but we see benefit in reducing the frequency of exposure to this type of advertising.
Cost-effectiveness	There may be some cost to platforms and businesses associated with compliance, particularly on forums that do not otherwise require age verification. Ongoing monitoring would incur expense to the Crown.
Intrusiveness	If implemented in the manner we envisage, we do not consider this initiative to be intrusive because it limits advertising of products to young audiences that they are already not legally allowed to purchase.
Speed of implementation	We expect that legislative changes to tighten online advertising restrictions could be implemented within 18 months. This could be considered in the design of the Government's approach to our other recommendations.
Comment	We consider that the onus should be on online platforms to ensure they take preventative and proactive steps to prevent young people from seeing advertising that is not age appropriate.

Recommendation

9. Restrict online advertising of alcohol, tobacco, and gambling
We recommend that the Government regulate to prevent online advertising of restricted goods to young people under the age of 18, in a way that aligns with the relevant offline advertising restrictions.

3.10 Educate and empower parents, guardians, and young people

As discussed previously in this report, we consider that parents and guardians have a responsibility to help keep young people safe online. However, we acknowledge that parents and caregivers often do not have access to resources on online safety, or do not know how to implement and maintain technical controls on their children's devices and platforms. We consider that the Government has a role to provide and share public safety information so that parents are better equipped to pass on accurate and informed advice to children and young people.

Existing tools to support parents to restrict online activity

A range of tools exist that can be used to assist parents and caregivers to keep their children safe from online harm. Tools such as parental controls were designed specifically for this purpose. However, parental controls can vary significantly between devices, operating systems, and platforms, and are often difficult to configure and maintain. Other available tools include:

- **Network filters provided by internet service providers (ISPs)**—Many large ISPs offer filters that block certain websites by intercepting the web traffic and checking it against restricted sites or terms that are captured by the filter.
- **Other commercial filtering products**—Several private companies such as Safe Surfer1 and the Crown-owned technology company Network for Learning (N4L) provide services including firewall and content filtering.
- **Device-level restrictions**—These are settings applied to a device's operating system that limit access to specific content or service on the device. They can be applied on smartphones, laptops, and tablets, and can be used by parents, schools, and workplaces.
- **Tools built into online platforms**—Many popular platforms provide a range of tools for parental controls, from limiting access to certain types of content, to offering specific account types for young people. These tools and account types would be more effective if there were a legislative requirement for age verification, as they are otherwise relatively easy to circumvent.

Device-level restrictions enable parents, educators, and caregivers to manage access to content, features, or applications on a certain device. Device-level restrictions can be implemented in two main ways: through operating system-level controls such as changing device settings, or by installing third-party apps onto devices. Some operators offer parental control features that can be used to change operating system settings on their devices.[27] These controls are more difficult to bypass or disable. Parents and caregivers can also choose to download third-party parental control applications on devices. These may be easier to circumvent as young people may be able to uninstall the apps. Network-level controls, such as network filters offered by ISPs, or internet router-based filtering, can be bypassed using a VPN or mobile data.

[27] For example: Apple Screen Time; Microsoft Family Safety; Google Family Link.

We have not reached a firm conclusion on what role government should play to promote or encourage the use of such controls. However, we consider that the Government should further consider ways to improve access and awareness of device-level and network-level controls, or empower a regulator to consider this topic further.

Barriers to effective parental responsibility

The uptake of existing tools is relatively low, likely due to a range of factors. Parents may not understand what tools are available or how to use parental controls. Households may also be concerned about the cost of commercial filtering products, or that such products may filter adults' internet access or slow the connection speeds.

Other barriers may include:

- socioeconomic factors such as knowledge of and access to technology
- the pace of new platforms and risks emerging, and parents' awareness of what their children, and children's peers, are likely to be accessing and sharing with each other
- parents overestimating their competency in managing their household's internet use and/or underestimating their child's technical savvy
- platform design decisions that are beyond parents' control
- peer pressure on young people
- difficulty protecting children from content when other parents and caregivers are not applying the same expectations or degree of restriction.

International approaches to supporting parents

Other jurisdictions have taken steps to ensure parents and caregivers have quality advice and resources, as well as requiring online platforms to implement safety measures to assist parents and caregivers to keep children safe.

In Australia, the eSafety Commissioner provides advice and resources for educators, parents, and young people.[28] Meanwhile, the EU's Digital Services Act requires online platforms to implement safety measures to protect young people, which includes implementing tools for verification and parental controls.

Our reflections on the need for greater support for parents

We consider that the Government should play a key role in minimising these barriers, and closing gaps in parents' knowledge and understanding. We acknowledge the effort and resources that the Government, businesses, and civil society organisations put into educating and supporting parents already. For example, we acknowledge the great work of the Keep It Real Online public awareness campaign, which began airing ads aimed at parents and caregivers from July 2020.[29] However, we believe more needs to be done, and more consistently across time and different population groups.

We also consider that platforms and internet service providers (ISPs) should do more to raise awareness of the parental controls and safety features they already have available. We

[28] Toolkit for Schools | eSafety Commissioner.

[29] Keep It Real Online.

strongly encourage platforms to give users clear information about safety features and make them a more visible part of their platforms.

At a minimum, we would like to see New Zealand implement an educational approach similar to Australia's. However, we consider the issue in New Zealand appears not to be the absence of options, or even information, but of ensuring that this information reaches the parents who need it most. We consider that education for parents needs to be prioritised by Government, and distributed so that it reaches all parents, including those in rural areas, those who speak English as a second language, and those who may not even have an online presence themselves.

If, as we understand it to be, there are households where the cost imposition of accessing suitable filtering products is a barrier to protecting young people, we would encourage the Government to consider how it might enable greater access to these tools.

Summary of our analysis: Education and awareness campaigns targeted at parents

Criteria	Our assessment
Proportionality	There is likely to be existing information that could be delivered through new channels or with greater effect to the audiences that need them most. This measure directly responds to many of the barriers we heard that parents face.
Cost-effectiveness	A national-level, comprehensive education campaign for parents and caregivers would incur some cost, but much of this may be drawn from existing resources depending on prioritisation across existing agencies.
Intrusiveness	We do not consider providing greater access to information to be intrusive. We note that the information provided should be action-oriented, evidence-based and culturally appropriate.
Speed of implementation	We see this as an ongoing need. However, educational and awareness campaigns at a national level could begin being delivered almost immediately, depending on resourcing and coordination across the relevant agencies.

Recommendation

10. **Educate and empower parents, caregivers, and young people**
    We recommend that the Government invest in public online safety campaigns or consider ways to fund the creation and promotion of comprehensive resources designed to educate and inform parents, caregivers, and young people about online safety.

3.11 Promote New Zealand-based research

Regulating requirements for algorithm design transparency would also open the door to a wider body of New Zealand-specific research. This could include longitudinal studies on some of the most worrying harms we have heard in evidence on this inquiry, harms caused

by long-term exposure to trends and body image competition online, as well as harms related to pornography, violence, and self-harm. We consider that the Government has a role to play in encouraging this research.

One of the key public benefits of a greater body of New Zealand-specific research into online harm would be to increase the amount of independent, empirical data on the subject. In our interim report, we stated our view that empirical research should be the foundation to inform policy development, ahead of anecdotal evidence. Increasing the body of research that evaluates the degree and prevalence of harm would aid a future regulator to better monitor the effectiveness of the interventions we recommend.

In addition to the international regimes we refer to elsewhere in this report, we also note that the UK's Online Safety Act empowers that Government to make regulations that require online platforms to provide information for independent research into online safety issues. Similarly, the EU's Digital Services Act also enables researchers to gain access to online platforms' data.[30] We would like to understand more about whether researchers in other jurisdictions have found such arrangements to be beneficial to their academic contributions.

Summary of our analysis: Promote New Zealand-based research

Criteria	Our assessment
Proportionality	Encouraging further New Zealand-specific research would provide a wider base for public discourse and future regulatory reviews.
Cost-effectiveness	Likely to be cost effective but may require research funding to be reprioritised from other areas.
Intrusiveness	We have not identified any concerns of intrusiveness for this proposal.
Speed of implementation	This could be established quickly. Ideally, we would hope to see an increasing volume of research begin from 2026 so that results of studies can start being published within the next two years. We would be particularly interested to see longitudinal studies commence as soon as possible, to build up an empirical evidence base to track trends over time.
Comment	To be effective, we consider that this would need to be progressed jointly with our recommendation on providing transparency of social media algorithms.

Recommendation

11. Promote New Zealand-based research

We recommend that the Government promote further research grounded in the New Zealand context, further deriving benefit from our recommendation to mandate algorithm transparency.

[30] New measures unlock access to data from largest online platforms to support research | European Commission.

4 Additional areas for consideration by Government

As noted in the introductory chapter of this report, one of the purposes of this inquiry has been to narrow the field of urgent, actionable policy decisions for the Government's consideration. This chapter sets out some of the key areas we recommend for further work, or as considerations in the design or implementation of our other recommendations.

We recommend that the Government take the following matters into consideration, either directly or by way of delegating them to the regulator:

Including young people in regulatory design

- **Consultation with young people—**We heard clearly from the young people who submitted to us that they want to be consulted in the design of interventions that affect them. Many of these submitters were in favour of the Government taking action to reduce online harm but expressed desire to be included in the development of solutions.
- **Education and digital literacy for young people—**We consider that there is a need to provide more educational resources to young people. However, we have not conducted detailed analysis or made a specific recommendation on this matter because we note that the national curriculum is being refreshed. We acknowledge the new curriculum is intended to include a stronger focus on online safety.

Reducing opportunity to evade restrictions

- **Virtual private networks (VPNs) as a means to evade restrictions—**We acknowledge there is well-founded concern that age restrictions on social media could be evaded by young people using VPNs. There is a very real risk of this in any situation where geo-blocking is the primary intervention. We recommend that this is an area for further exploration by the regulator.
- **Device-level restrictions—**We consider device-level restrictions to be one of the most promising avenues for limiting young people's access to harmful content. We have not reached a conclusion on the most appropriate role for Government to play in encouraging the uptake of devices with limited functionality, or restricting the use of certain personal devices. However, we recommend that this receive further consideration because device-level restrictions appear to be more difficult for young people to bypass. We recommend that the regulator be empowered to consider this topic further.
- **Collaboration with online platforms to limit VPN use—**We are aware that online platforms may share our interest in limiting users' ability to use VPNs to bypass any restrictions on using their platforms. We encourage the Government to explore this further.
- **Collaboration with cell and internet service providers—**We believe there are further opportunities to work with cell phone companies and internet service providers, both to make the most of existing harm-prevention tools and to implement new ones.

Minimising privacy risk and intrusion on rights and freedoms

- **Age-verification technology—**We understand there is nascent technology that could assist in age verification without the need for a person to verify their identity or provide other personal details. We encourage further exploration of this as an emerging, albeit as yet imperfect, potential solution to some privacy concerns.
- **Freedom of expression**—We acknowledge that many of our proposals could be seen to infringe on freedom of expression. We do not take this lightly and after much consideration have concluded that age restrictions on social media would be proportionate to the harm being addressed. Nonetheless, we acknowledge that the Government would need to take this into account in the process of preparing its response and future interventions.

Reviewing the approach to labelling

- **Online gambling**—We heard that online gaming can be a significant part of young people's lives. In addition to restricting or prohibiting certain types of content, the Films, Videos, and Publications Classification Act also provides a framework for assessing and classifying commercial video content. This supports people to make informed decisions about consuming video content, both for themselves and for those in their care. The Act's definitions do not map well to current technologies. For example, the definition of "video games" only includes physical video games, not online video games. Online video games are not currently required to be classified or labelled under the Act.
- **Platform labelling**—We heard that New Zealand has an existing framework for content labelling but that this has not been kept up to date with the ways that content is created, distributed, and accessed by young people online. There may be options to provide classifications for online platforms, rather than individual pieces of content. We understand that this approach may require changing the Chief Censor's mandate.

Updating offences and penalties

- **Sentences for grooming**—There are two offences for grooming under the Crimes Act. The offences are described in section 131AB (Grooming for sexual conduct with a young person) and section 131B (Meeting young person following sexual grooming, etc). We have been advised that the offences and penalties were reviewed in 2023 when section 131AB was inserted into the Act, but that there are no plans for further amendments to grooming offences.
- **Sentences for stalking and harassment**—We heard from submitters who were concerned about online platforms enabling stalking and harassment. Offences for stalking and harassment were added to the Crimes Act through the Crimes Legislation (Stalking and Harassment) Amendment Act 2025. The Crimes Act now contains provisions to cover digital communications used in this way. Offences apply for young people (aged 14 years and over) as they do for adults, but youth offending is dealt with in the youth justice system rather than the adult criminal justice system.

Accessibility considerations

- **Access to information in te reo Māori and other languages**—We see a need for greater engagement across population groups about online harm, in particular to equip

parents and caregivers with the tools they need to protect the young people in their care.

- **Government support for household network filter technologies—**We encourage the Government to undertake further analysis of whether there are real financial constraints to parents and caregivers obtaining products that can prevent young people from accessing harmful online content at home, and how it could respond if so.

Recommendation

12. Consider further matters

We recommend that the Government consider each of the matters set out in Chapter 4 of this report and/or task them to the regulator recommended above to further consider, as appropriate.

5 Conclusion

We consider that online safety, particularly for children and young people, is of paramount importance. We have recommended a range of actions to strengthen and improve the ways in which young people are kept safe online.

We would like to thank the 400 individuals and organisations, and particularly the children and young people, who made a submission to our inquiry. Although we summarised the submissions we received in more detail in our interim report,[31] the voices and life experiences of submitters have also helped inform our final recommendations in this report. We have heard directly from young people who are concerned about the harms that they or their peers experience. We are deeply concerned about the degree of social, psychological, and physiological harms that are occurring, and thank submitters for sharing their experiences with us.

We recognise that further evidence and analysis would be needed before many of our recommended actions are implemented. Nevertheless, the majority of us strongly believe that intervention is necessary to protect young people from harm right now. Although some of our individual recommendations may be challenging to implement, this does not mean they should not be pursued and considered further. We recognise that there are concerns that young people could evade restrictions designed to keep them safe, such as age restrictions on social media. While some young people may find ways to bypass age restrictions, we consider that such an intervention would be likely to strengthen protection for younger children, and would encourage discussions and education about digital safety.

We consider that the implementation of our recommendations, or the design of any other digital regulation, needs to consider flexibility so that New Zealand's response is able to adapt to new evidence or emerging technologies. We consider that an independent regulator would be best placed to advise decision-makers on proportionate interventions and regulation. If established, we encourage the regulator to give further consideration to many of the topics explored in our inquiry.

We note that the Government is required to respond to our recommendations within 60 working days after this report was presented (by 3 June 2026). We look forward to seeing the response and intend to follow up on the Government's consideration. Overall, we urge the Government to take urgent action to keep children and young people safe from online harm.

[31] Inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in addressing those harms | Education and Workforce Committee.

6 Differing views

6.1 Green Party of Aotearoa New Zealand differing view

The Green Party is thankful that the Education and Workforce Committee has progressed this important inquiry, and broadly supports the recommendations made.

It is clear that there is significant harm caused, not just to young people, but to all users of social media platforms. Users are subjected by design to a wide range of content that can harm mental health and deepen social polarisation. We are pleased that the inquiry has made a range of credible and proportionate recommendations to address this harm.

We particularly support establishing an independent national regulator, strengthening the liability of platforms for harm, prohibiting “nudify” apps, regulating algorithmic recommendation systems, mandating algorithm transparency, and restricting online advertising of restricted goods to young people.

Our view is that the big social media platforms must be held accountable and made responsible for harm and safety on their platforms, and that should be the priority for regulatory efforts to address online harm.

Age restrictions

The Green Party maintain ongoing concerns with the recommendation to restrict social media access for under 16-year-olds. We do not believe restricting access to social media for under 16-year-olds would address the concerns identified.

We have heard from under 16-year-olds across the country that they do not think the proposal to restrict social media access will deter the behaviour it intends to address, and that young people will find ways around these rules. On the other hand, we have also heard from concerned parents who are worried about their children’s safety and mental health as a result of social media use.

Effective age restriction requires all users to provide personal identification to social media platforms, that already cannot be trusted to protect user information. We are sceptical that age restriction technology that does not infringe on the privacy of all users and is effective at preventing minors from accessing social media platforms exists.

We are also concerned that age restrictions could drive youth from regulated platforms to other fringe, unregulated, and harmful platforms, undermining the purpose of age restrictions.

Many submitters also noted the importance of online spaces for marginalised communities, particularly LGBTQ+ and disabled youth, and were concerned about the impact of proposed age restrictions on communicating with their peers and support networks.

We support strong regulation to fix the platforms and the harmful content their algorithms promote for all users, rather than preventing young people from accessing regulated social media platforms that they value and driving them to less safe parts of the internet.

VPNs

We are also concerned with the recommendation for the national regulator to explore how to stop the use of VPNs (Virtual Private Networks) to evade age restrictions. VPNs are legitimately used by a range of users to protect their data and privacy. The proposal to control VPNs has deeply complex implications for security and control of personal and business information.

It would be technologically impossible for regulated digital platforms to block VPN users from New Zealand, who would otherwise have to block all VPN users around the world—including those using VPNs to bypass internet censorship by authoritarian governments. This recommendation is misguided.

6.2 ACT New Zealand differing view

In 2025, ACT MP Dr Parmjeet Parmar wrote to the Education and Workforce Committee seeking an inquiry into the impacts of social media on young people. ACT supported this inquiry because we believe Parliament should take the time to clearly define the problem, test the evidence, and consider the real-world consequences of any proposed solution before rushing into regulation.

The committee was tasked with examining the harm that young New Zealanders encounter online and identifying proportional and actionable interventions to address those harms. This committee, in its recommendations, has substantially failed to do this and, worse, has proposed measures that expand government overreach through new regulators with unclear mandates, effectively endorsing a framework requiring New Zealanders to provide their ID digitally, and raising the spectre of regulating the very tools that protect New Zealanders' privacy.

The concept of a ban is a simple one; the breadth of the recommendations underlines the lack of seriousness this committee has taken in looking at the workability of such a ban.

Australia's ban, despite its relatively simple approach, has had the unintended consequence of weakening existing safety protections for young people. YouTube offered to share its experience with the committee, but that offer was unfortunately and unwisely declined.

ACT is deeply concerned that the committee declined to seek advice from the Department of Internal Affairs on age restrictions for social media platforms, despite the inquiry being centred on that very issue. ACT is disappointed and embarrassed that the committee had a lack of understanding of the role of select committees and their relationship with the executive. The legislature's responsibility is to scrutinise and hold the executive to account. Whether or not the Government was reportedly progressing legislation in this area should have been irrelevant and given that the committee's final report included a recommendation to ban social media for under-16s, it should have been incumbent on members to obtain the relevant departmental advice. The refusal to do so reflects a lack of seriousness and diligence of an inquiry with significant and far-reaching implications.

ACT believes that there is real potential harm on social media for young people. We understand the concerns parents have when it comes to young people online. ACT believes those concerns deserve to be taken seriously and deserve to be explored thoroughly.

Recommendation to ban social media for under-16s and "age verification"

ACT is concerned by recommendations that move towards banning social media for those under 16. While the intention to protect young people is well meant, the evidence presented to the committee, along with international experience, shows that such a ban would be difficult to enforce without requiring widespread age verification.

In practice, enforcing an age-based social media ban would require all New Zealanders to prove their age online, something the report notes where it says such a ban would "likely involve sharing proof of identity". This would not be limited to young people. Adults would also be required to verify their identity in order to access everyday online services.

ACT is concerned that this approach represents a significant step towards requiring people to provide identity online. ACT does not support any move that would require New Zealanders to provide identification to social media companies routinely. Protecting young people online must not come at the cost of reduced privacy, increased surveillance, or the erosion of personal freedoms for everyone else.

ACT believes that working on responses requiring the likes of digital ID for age verification should not be the priority of the Government, and instead the Government should focus on a sophisticated and carefully considered response. Addressing these issues effectively is likely to require a combination of measures, potentially including strengthened digital literacy in schools, better support and education for parents, and, where appropriate, proportionate regulatory settings.

ACT also believes education should extend to young people so that when they access social media, they are able to recognise the potential harms and avoid them while also being able to recognise the potential benefits.

However, ACT does not consider that sufficient time or analysis has been devoted to investigating and fully evaluating these alternative approaches. Instead, it seems the committee reached a predetermined approach prior to any evidence being presented. Before adopting a significant intervention such as banning social media for under-16s requiring age verification including potentially a digital ID system, the Government should ensure that a full range of options has been properly explored and assessed.

VPNs

ACT is concerned with the committee's recommendation that the regulator explore how to stop the use of Virtual Private Networks (VPNs). VPNs are legitimate privacy and security tools used by businesses, journalists, and everyday New Zealanders to protect their data online. They are an essential tool for cybersecurity.

Proposals to look at the regulation of VPNs or to establish a new regulator should be seen as what they are—a failure to properly engage with how a ban would work in practice and proportionally balance a ban against the rights of New Zealanders.

The idea that the Government should explore a regulator having any authority over VPN use shows the lack of seriousness some committee members took regarding the inquiry. The ability to restrict New Zealanders' access to the internet is not something the committee was asked to explore, nor should it have.

ACT believes the committee members who support such a move should recognise that the countries that have placed restrictions on VPNs include North Korea, China, Russia, Turkmenistan, and Iran. These countries use these restrictions to suppress their citizens' free speech, often in the name of protecting from online harm.

If these committee members truly believe that these countries are a good example of internet safety, it shows the lack of direction the committee took when exploring its options. Rather than focusing on a ban or even broadly what the committee was asked to do, it sought to push forward untested ideas that simply take away New Zealanders' privacy with no clear reason provided.

National regulator

ACT firmly rejects the idea that the answer to the simple concept of a social media ban is a complex regulator.

New Zealand is already governed by a maze of regulations in this space. While the committee proposes some fixes to make it clearer and concise, it seems the committee's instinct was not protection for young people, but rather to build a new feel-good bureaucratic mess because regulation is easier than good leadership.

The international examples given in the report should have given members of the committee some concern about whether a national regulator was the right approach, but instead, these examples seem to have been conveniently ignored, even when submitters from those countries laid them out plainly.

In both the United Kingdom, with Ofcom, and Australia, with the eSafety Commissioner, there have been clear and consistent criticisms of overstepping and opaque processes, which have eroded public trust that the Government’s goal is to uphold free expression. The Free Speech Union in the United Kingdom made a serious effort to be heard, yet the recommendation does not heed any concerns and instead says that New Zealand could borrow design features from those jurisdictions. It is unclear if the report means New Zealand should borrow the serious breach of free speech or the massive crackdown on freedom of expression.

Before Parliament creates a powerful new regulator with the authority to police speech and take away New Zealanders' privacy, there must be a clearly defined problem that cannot be addressed through existing frameworks. ACT has not seen that case made.

Banning deepfake apps

ACT unequivocally opposes the creation of sexually explicit deepfakes. We find the practice abhorrent and believe those who create and distribute non-consensual deepfake material should face serious consequences.

However, ACT is concerned that the committee’s recommendation focuses on banning so-called “nudify apps”, a term that has not been clearly defined. Attempting to prohibit software categories without precise definitions risks unintended consequences and legal uncertainty.

The appropriate response is to criminalise harmful behaviour, namely, the creation and distribution of non-consensual sexually explicit content, rather than attempting to ban

technology itself. Laws should target those who misuse technology to harm others, not the underlying tools that have legitimate applications.

Mandating algorithm transparency

ACT is concerned that the recommendation to give a regulator power to require information from platforms relating to their algorithms, as well as provide researchers with information about algorithmic design, is unnecessary and risks compromising commercially sensitive information. Algorithmic systems are often proprietary technologies that companies have invested heavily in developing. Forcing disclosure may undermine competitiveness and discourage investment in New Zealand's digital economy.

Overall

ACT believes that the committee's recommendations steer away from protecting young people and, unfortunately, towards proposing a requirement for people to share their ID digitally and new regulation to fix the issues. The goal of protecting young people should not come at the expense of all New Zealanders' right to privacy.

ACT believes that the committee's terms of reference for the inquiry made it clear what the goal was. We believe that the committee has categorically and embarrassingly failed in this, going well beyond its remit, seeking solutions before identifying the true problem. An exploration of a social media ban is simple, yet the committee made a complete mess of it.

It is easy for the committee to say in its report that it does "not take this lightly" when it comes to free speech and expression, but it is clear these words were an afterthought rather than central to the committee's recommendations.

New Zealand should utterly reject being a "fast follower" if we are heading towards the erosion of privacy and expansion of the state peering into the legitimate online behaviour of our citizens.

Inquiry into the harm young New Zealanders encounter online

Education and Workforce Committee

March 2026

What we heard	What we recommend
Current laws are not fit for purpose	• Address legislative gaps • Establish an independent national regulator for online safety
Online harm is serious and widespread	• Review platforms' liability for harm resulting from the content they host and the platform design
Harm can affect mental health, wellbeing, and development	• Introduce age restrictions for social media platforms
Deepfake technology can be misused to create fake sexual images that cause serious harm	• Ban "nudify" apps and prohibit the creation and distribution of non-consensual deepfake sexual imagery • Regulate deepfake technology
Algorithms can push harmful or extreme content	• Consider regulating algorithmic recommendation systems
The design of online platforms can cause or exacerbate harms	• Explore mandating algorithm transparency • Promote New Zealand-based research
Young people are exposed to harmful advertising	• Prevent online advertising of alcohol, tobacco, and gambling for under 18s
Parents want to help but lack clear support	• Educate and empower parents, caregivers, and young people

More work needs to be done

This report is a part of an ongoing national conversation about how to respond to online harm in New Zealand. The committee agreed to some of its recommendations unanimously. However, members, like submitters, have a range of views on how to address these problems. This range of views is indicated in the report. The Government must respond to the recommendations by 3 June 2026.

Some areas for further exploration include:

- Including young people in regulatory design through consultation
- Reducing the opportunities to evade restrictions
- Government support for device-level and network-level parental controls
- Education and digital literacy for young people
- Updating offences and penalties for grooming, and stalking and harassment
- Access to information in te reo Māori and other languages
- Minimising privacy risk and intrusion on rights and freedoms

Appendix A: Committee procedure

Committee procedure

We met between 4 June 2025 and 4 March 2026 to consider the inquiry. We called for public submissions with a closing date of 30 July 2025. We received submissions from 400 organisations and individuals and heard oral evidence from 87 submitters. We received advice from the Department of Internal Affairs.

Committee members

Katie Nimon (Chairperson)
Carl Bates (Deputy Chairperson)
Shanan Halbert
Francisco Hernandez (until 11 February 2026)
Grant McCallum
Dr Parmjeet Parmar
Hon Willow-Jean Prime
Hon Phil Twyford
Dr Vanessa Weenink (Acting Chairperson from 16 July to 8 August 2025)
Dr Lawrence Xu-Nan (from 11 February 2026)

Mike Butterick, Reuben Davidson, and Hūhana Lyndon also participated in our consideration of this inquiry.

Related resources

The documents we received as advice and evidence for this inquiry are available on the Parliament website, along with recordings of our hearings:

- 6 October 2025 (video 1).
- 8 September 2025 (video 1, video 2).

Appendix B: Terms of reference

The Education and Workforce Committee will undertake an inquiry into the harm young New Zealanders may be exposed to online.

Aims

It is intended that the inquiry will:

- examine the nature, severity, and prevalence of online harm experienced by young people in New Zealand, including but not limited to online bullying, exploitation, addictive use, mental health impacts, educational impacts, and exposure to harmful content
- recommend, where appropriate clear and actionable solutions to clearly identified problems after comparing them against both the problems and the benefits associated with online activity—any recommendation should be assessed for proportionality, including the efficacy, workability, severity and likelihood of harm, cost-effectiveness, intrusiveness, and coerciveness.
- consider the speed and practicality by which any recommendations would be able to be implemented.

Consideration

We will conduct the inquiry taking into account the following context:

- note that not all young people experience the world in the same way, and there may be a range of experiences online for different young people, and they are all valid perspectives
- potential solutions could have roles for all, or combinations of, Government, business, including social media companies, and civil society, including parents and children.

Approach to the inquiry

To understand the problem, we will:

- consider the social, educational, and developmental benefits that online activity may offer to young people, and the extent these benefits are realised
- review current harm reduction measures and interventions undertaken by Government, educators, parents and caregivers, community organisations, and social media companies
- seek a range of views, which may include:
    - parents, caregivers and young people
    - relevant community organisations
    - relevant medical and psychological practitioners and experts
    - educators
    - technology experts
    - overseas policymakers involved in addressing similar harms
    - government departments

    - social media companies
- evaluate the effectiveness of existing measures in reducing the incidence and severity of online harm among young people
- assess whether the limitations of current harm reduction efforts are primarily due to design, resourcing, or lack of uptake and engagement
- determine whether additional or alternative measures are warranted
- consider any other matters the committee deems relevant as the inquiry progresses.

Management of the inquiry

We will:

- receive written submissions from any interested individuals or organisations
- hold oral hearings by invitation, potentially in tranches, in order to ensure both a diversity of views and value adding contributions to the committee's role
- work to a schedule that enables reporting to the House by the end of November 2025.

Appendix C: Further resources and resources

Resources for young people

- Advice for children and young people on online safety | Netsafe.
- Social media safety | Netsafe.
- Hector's World: Videos on online safety for children in Years 0–6 | Netsafe.
- Keeping me safe with parental controls | Classification Office.
- The Bare Facts: The reality of sharing online intimate images | Classification Office.
- What is objectionable content? | Classification Office.
- Algorithms 101 | Classification Office.

Resources for parents and caregivers

- Advice for parents and caregivers on online safety | Netsafe.
- Online safety | Department of Internal Affairs.
- How to keep your family safe online | Department of Internal Affairs.
- Guide to parental controls available in New Zealand | Classification Office.
- Video on how to use parental controls | Classification Office.
- How to talk with young people about pornography | Classification Office.
- Illegal and harmful content: resources for supporting young people | Classification Office.
- How do we talk with our kids about seeing harmful content online? | Classification Office.

Research on young people's online experiences in New Zealand

- Children and youth online safety in Aotearoa New Zealand | Netsafe and Save the Children (2025).
- New Zealand children's experiences of online risks and their perceptions of harm | Netsafe (2020).
- Growing Up with Porn: interview research on young New Zealander's experiences with porn online | Classification Office (2020).
- Content that Crosses the Line: Conversations with young people about extremely harmful content online | Classification Office (2025).
- Digital Reflections: The Online Experience and its Influence on Youth Body Image in Aotearoa | Classification Office and Netsafe (2024).
- Factsheet: The digital parenting strategies and behaviours of New Zealand parents | Netsafe (2021).
- Aotearoa Internet Insights | InternetNZ (2024).