



**New Zealand House of Representatives**  
Te Whare Māngai o Aotearoa

**Education and Workforce Committee**

Komiti Whiriwhiri Take Kuranga, Take Hunga Mahi

54th Parliament

December 2025

---

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

Interim report

---

## Contents

Recommendation.....	3
1 Introduction.....	3
1.1 Inquiry purpose and terms of reference .....	4
1.2 Our process for conducting this inquiry .....	5
1.3 Structure and nature of this report .....	6
2 Online harm experienced by young New Zealanders .....	7
2.1 Online harm.....	7
2.2 Experiences shared with us .....	11
2.3 Research and understanding of online harm .....	15
2.3 Our response and reflections.....	16
3 Approaches to addressing online harm in New Zealand.....	18
3.1 Current legislative and regulatory settings .....	18
3.2 Roles and responsibilities of online platforms .....	22
3.3 Roles and responsibilities of parents, educators, and civil society .....	26
3.4 Our response and reflections.....	28
4 International experiences .....	30
4.1 Summary of experiences in similar jurisdictions.....	30
4.2 Social media age restrictions .....	35
4.3 Algorithm transparency.....	35
4.4 Our response and reflections.....	36
5 Our overall reflections and next steps .....	37
Green Party of Aotearoa New Zealand differing view .....	40
ACT New Zealand differing view .....	40
Appendix A: Committee procedure.....	42
Appendix B: Terms of reference.....	43
Appendix C: Further resources and resources .....	45

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

## **Recommendation**

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. The committee recommends that the House take note of its interim report.

## **1 Introduction**

The internet has introduced new ways in which people can connect, share stories, purchase goods, and find information. It has also exacerbated ways in which people can be hurt, and created new forms of harm. Our inquiry examines the harm young New Zealanders encounter online, and investigates the roles that Government, business, and society should play in addressing those harms.

The purpose of our inquiry is to examine the nature, severity, and prevalence of online harm experienced by young New Zealanders and make recommendations for clear and actionable solutions. In this interim report, we summarise information and advice we have received relating to young people's experiences of online harm, and provide an overview of current efforts to address online harm in New Zealand. We also indicate where, either unanimously or by majority, the committee has agreed action should be taken and/or intends to undertake further consideration. We intend to produce a final report in early 2026 assessing potential solutions and making recommendations to the Government.

We emphasise that there is still a lot of work ahead for us to understand the full range of experiences that young people have online and identify effective, enduring, and clear solutions. We hope that this interim report, and ultimately our inquiry as a whole, will contribute to discussions and decision-making processes to inform how New Zealand responds to these challenges.

## 1.1 Inquiry purpose and terms of reference

### Terms of reference

We initiated this inquiry on 4 June 2025. On 25 June, we adopted terms of reference to guide our work.

In our terms of reference, we set out that we aim to:

- 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 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.

We also noted our intention to conduct the inquiry taking into account the following context:

- 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 of, or combinations of, Government, business, including social media companies, and civil society, including parents and children.

We also set out how we planned to consider, approach, and manage the inquiry. The full terms of reference are available in Appendix B (*see pp 43–44*).

Not all topics included in our terms of reference are discussed in detail in this report. Other topics will be elaborated on in our final report.

### Context for our inquiry

We hope to contribute to current discussions and policy decisions relevant to online harm. In May 2025, Catherine Wedd MP put forward a member's bill that would restrict access to social media platforms for under 16-year-olds.<sup>1</sup> The bill would require social media platforms to take all reasonable steps to prevent under 16-year-olds from holding an account with them. Following this, the Prime Minister indicated that the Government would progress work to restrict access to social media for under 16-year-olds. He instructed the Minister of Education to look into this topic.

In May 2025, Laura McClure MP also put forward a member's bill proposing to criminalise the creation, possession, publication, and sale of sexually explicit deepfakes.<sup>2</sup> Deepfakes are images, videos, or audio that depict a person's likeness and have been digitally altered using technology like artificial intelligence.

---

<sup>1</sup> [Social Media \(Age-Restricted Users\) Bill | New Zealand Legislation](#).

<sup>2</sup> [Deepfake Digital Harm and Exploitation Bill | New Zealand Legislation](#).

On 23 October 2025, both of these bills were drawn from the members' bill ballot and introduced to Parliament.<sup>3</sup> We hope that our inquiry can contribute to, and help inform, the discussions by the public and Parliament on these bills.

## **1.2 Our process for conducting this inquiry**

We initiated this inquiry on 4 June 2025. On 29 July, we appointed the Department of Internal Affairs (DIA) as advisers to assist with our consideration. We also received advice from the Parliamentary Library during our consideration.

Dr Parmjeet Parmar MP wrote to us on 6 May 2025 to propose that we initiate an inquiry into reducing the harms of social media on young people. We initially opened a briefing on 14 May 2025 about the harm young New Zealanders encounter online. However, this topic did not directly relate to our remit as the Education and Workforce Committee, which is to examine matters related to education, training, employment, immigration, industrial relations, health and safety, and accident compensation. We decided to close the briefing and sought the Business Committee's support for a notice of motion asking the House of Representatives to authorise us to undertake an inquiry on this subject. A members' motion from our Deputy Chairperson, Carl Bates MP, was agreed to by the House on 21 May 2025.

We invited public submissions on this inquiry from 26 June to 30 July 2025. We received 430 submissions from 400 individuals and groups.<sup>4</sup> They covered a range of viewpoints, including young people, parents and caregivers, children and youth groups, community representative groups, current regulatory bodies, digital or online safety groups and representatives, social media companies, educators, academics, and researchers. A total of 285 individuals made submissions. DIA provided a thematic analysis of the submissions, identifying different perspectives and common themes expressed by submitters. We held public hearings on 8 September and 6 October 2025, meeting with 87 groups and individuals.

We would like to thank everyone who made a submission and attended our hearings. We appreciate submitters sharing their time, experiences, and expertise with us. In particular, the breadth and depth of the views shared was exceptional. We also want to specifically acknowledge the personal stories that children and young people shared with us about the harm they have encountered online, as well as the benefits they feel being online provides. Similarly, we thank parents and caregivers who shared concerns about their children's experiences online.

In our terms of reference, we noted our intention to provide a final report on our inquiry by November 2025. Reflecting the amount of evidence received and the high quality of submissions, we decided instead to provide our report in two parts. After this first, interim report we intend to produce a final report in early 2026.

---

<sup>3</sup> Members' bills are bills that can be introduced by any member of Parliament who is not a Minister. Ballots are held to decide what members' bills will be introduced to be debated in Parliament.

<sup>4</sup> The number of submissions is higher than the number of submitters as some submitters also provided supplementary submissions or supporting material.

Our final report will focus on our analysis of potential solutions, interventions, or legislation that could be introduced to address the harms young New Zealanders encounter online. In that report we intend to make recommendations to the Government on ways to address online harm.

### **1.3 Structure and nature of this report**

The intention of this interim report is to summarise the main themes from submissions and advice we have received so far. We hope that, in doing so, we can highlight the valuable insights from submitters and contribute to ongoing discussions about how New Zealand can address harm from online spaces. In this report, we indicate our initial views and the topics we intend to consider further in our final report. While our comments reflect the direction we intend to travel with this inquiry, final conclusions will be included in our final report. We do not offer solutions or recommendations in this report. Rather, we provide an overview of young people's experiences of online harm, the effects that these harms have on young people, and the risks and factors that contribute to these harms. We also outline the current ways in which online harms are addressed in New Zealand, including relevant law, educational resources, and online safety mechanisms.

Each chapter of our report has roughly the same structure. First, we summarise some of the information received from public submissions and advice. We then provide our thoughts on the topic. In our conclusion, we summarise our preliminary suggestions for solutions to be investigated and the topics we intend to explore further in our final report.

The inclusion of information from the public and advisers in this report should not be treated as an endorsement of any views. It is simply an account of the key material that we received. The opinions and reflections of this committee as a whole, or of individual members of this committee, are expressed only in this introduction, chapter 5, and the *Our response and reflections* sections at the end of each chapter.

## 2 Online harm experienced by young New Zealanders

### 2.1 Online harm

Submitters were generally in agreement that young people in New Zealand are experiencing substantial harm from their use of, or experiences on, online platforms. Children and young people themselves shared personal stories with us of harm that they had experienced in online spaces. Submitters described a wide range of types of harms that young people can experience, including exposure to child sexual abuse material and depictions of violence, cyberbullying, and being targeted by coercive advertising.<sup>5</sup>

We heard that these types of harmful exposure online could have different effects on young people, including psychological, physical, developmental, and social effects. Many submitters also commented that the design of online platforms, such as social media or apps, influence the experiences young people can have online, and that some design features can contribute to harm.

In contrast, some submitters also discussed the benefits that online environments can bring to young people's lives. In particular, submitters highlighted the benefits of online spaces offering connection, access to mental health resources, safe environments for young people to explore their identities, and opportunities for activism.

While our report focuses on online harm, we acknowledge that there are many advantages of online platforms and access to the internet that can benefit young people. In assessing any proposed solutions to address online harm, we intend to also consider the social, educational, and developmental benefits that online activity may offer to young people, and the extent to which these benefits are realised.

### Defining “online” and “young New Zealanders”

We define “young New Zealanders” as children and young people who live in New Zealand and are under the age of 24. Submitters spoke about the online experiences of children and young people from a range of ages, including very young children.

The scope of our inquiry covers all online content and activity conducted over the internet. This includes, but is not limited to, young people's experiences using instant messaging platforms, app stores, video-sharing platforms, search engines, internet service providers, cloud-based storage services, gaming platforms, streaming services, artificial intelligence (AI) and chatbots.

---

<sup>5</sup> Child sexual abuse material or child sexual exploitation material generally refers to a recording of the sexual abuse or exploitation of a child or young person.

## **Defining “social media” platforms**

The majority of submitters commented on issues or concerns related to young people’s experiences on social media and online gaming platforms specifically. Multiple definitions for social media are used across different disciplines and for different contexts. As such, there is no single definition, and as new platforms emerge, these definitions may change.

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.

We do not include instant messaging platforms in our definition of social media. Instead, in this report, we use the term “online platform” to encompass a broader range of digital platforms, websites, and apps. This may include social media, instant messaging platforms (like Facebook Messenger and WhatsApp), media-sharing platforms (like YouTube, Vimeo, or Spotify), streaming platforms (like Twitch and Discord), and e-commerce websites and platforms (like Amazon or Etsy).

Because of the focus from submitters, much of our discussion in this chapter relates to social media platforms. However, the reflections we make, and the eventual recommendations we plan to make in our final report, are not necessarily limited to experiences on social media platforms.

## **Defining “online harm”**

Online harm is a difficult term to define. It is a complex issue with overlapping legal, social, psychological, and technological aspects. We understand that exposure to different forms of content or activity online can affect young people in different ways—what causes harm to one young person may not necessarily be distressing to others. We heard that factors such as age, developmental stage, cultural background, social and family context, psychological wellbeing, and socioeconomic circumstances can all influence how young people experience online environments. As the online environment and emerging technologies, such as generative AI, evolve rapidly, the risks that they present to young people also evolve. This makes both understanding and addressing online harm a difficult task.

For this inquiry, we treat “online harm” as an umbrella term that encompasses both the exposure to harmful content or activity online and the effects of this exposure. We frame the issue as twofold. Submitters described both a wide range of types of content, behaviours, and activities that can cause harm, and a wide range of potential impacts that exposure to this material can have on young people. For example, exposure to harmful content such as depictions of violence may cause immediate emotional harm, and may also contribute towards ongoing psychological effects on mental health.



## Types of harm

In this report, we use the online safety framework introduced in the United Kingdom's *Keeping children safe in education* guidance to classify different types of online harm.<sup>6</sup> The framework categorises four types of harm:

- **Content harm**—exposure to harmful or inappropriate content shared deliberately or unintentionally, such as child sexual abuse material, adult content like pornography, violent or graphic content, or content related to self-harm, suicide, or eating disorders.
- **Contact harm**—exposure to harmful or unsafe online interactions with others such as grooming, online stalking, and sexual exploitation.
- **Conduct harm**—the intentional use of online platforms to harm or abuse a user or group of users, such as cyberbullying, doxxing, and sextortion.<sup>7</sup>
- **Commerce harm**—harmful online commercial activities, such as scams, advertising of commodities such as alcohol, drugs and vaping, or inappropriate advertising that exploits users and undermines their safety and trust.

We understand that these harms often overlap and that experiences shared by submitters were also sometimes broader than these categories. For example, submitters explained that ongoing exposure to content about other people's achievements or appearance can influence young people's self-esteem. While this may not in and of itself be classified as harmful content, we heard plentiful evidence that prolonged exposure to it may harm young people.

## Potential harmful effects

Submitters also discussed how online harm can have potential psychological, physical, developmental, and social and relational effects. For example, submitters expressed concern that online activity may contribute to:

- poor mental health, including increasing anxiety or depression
- behavioural issues or emotional dysregulation
- injury to self
- poor sleep
- reduced attention span or focus leading to poor learning outcomes
- addictive use of digital technology or social media
- strain on parental and familial relationships
- harmful behaviours in social and intimate relationships.

We discuss the extent of research available on the effects of online activity later in the report (see pp 15–16).

---

<sup>6</sup> [Keeping children safe in education | United Kingdom Government.](#)

<sup>7</sup> Doxxing refers to revealing sensitive, secret, or personally identifiable information about someone online. Sextortion is a form of blackmail that involves threatening to reveal sexual or intimate personal images of the victim online.

## Types of Harm

Content	Conduct	Contact	Commerce
<ul style="list-style-type: none"> <li>• Illegal (sexual abuse, serious violence and crime, stalking)</li> <li>• Dangerous (self-harm, dangerous challenges)</li> <li>• Manipulation (extremism, misogyny, disinformation)</li> <li>• Adult only (pornography)</li> </ul>	<ul style="list-style-type: none"> <li>• Sharing personal information</li> <li>• Sexting, nudes, deepfakes, sextortion, image-based abuse</li> <li>• Harmful groups</li> </ul>	<ul style="list-style-type: none"> <li>• Grooming</li> <li>• Cyberbullying</li> <li>• Harassment</li> <li>• Unwanted contact</li> <li>• Doxxing</li> </ul>	<ul style="list-style-type: none"> <li>• Scams</li> <li>• Gambling</li> <li>• Inappropriate advertising</li> <li>• Children accepting terms and conditions or online contracts</li> </ul>

All types of harm feed into all potential effects

## Potential Effects

Psychological	Physical	Developmental	Social & Relational
<ul style="list-style-type: none"> <li>• Low self-esteem</li> <li>• Anxiety / depression</li> <li>• Self-harm</li> <li>• Trauma / PTSD</li> </ul>	<ul style="list-style-type: none"> <li>• Injury to self</li> <li>• Injury to others or their property</li> <li>• Sleep disruption</li> </ul>	<ul style="list-style-type: none"> <li>• Emotional dysregulation</li> <li>• Focus and attention issues</li> <li>• Identity formation issues</li> </ul>	<ul style="list-style-type: none"> <li>• Relationship breakdown</li> <li>• Social isolation</li> <li>• Trust issues</li> <li>• Social cohesion</li> </ul>

Figure 1: Types of harm and potential effects identified by submitters

## Online platform design and features

We heard that online harm can result not just from the content and activity young people interact with online, but also from the features or design of online platforms themselves. The design choices of digital media platforms—such as the user interface, algorithms, levels of customisation, and user controls and settings—are not neutral. Technological design choices can influence how users experience the digital environment. Design and features may influence, incentivise, or constrain certain forms of engagement depending on what kind of options are presented to people. Often, platforms’ design choices are informed by their business models and commercial goals.

Submitters were concerned that elements of the design of online platforms prioritised user engagement over safety. For example, submitters expressed concern that:

- recommendation algorithms and infinite scroll features, enabling a user to browse content endlessly, can contribute to addictive use of social media
- short-form videos, common on Instagram Reels and TikTok, may reduce attention spans
- algorithms may amplify harmful and shocking content or mis- and dis-information<sup>8</sup>
- beauty filters, that allow users to modify their appearances in images or videos, may affect young people’s self-esteem and reinforce harmful beauty standards
- features of mobile or digital games, such as loot boxes or gacha mechanics, expose young people to gambling-like behaviours.<sup>9</sup>

Some submitters also expressed concern about the level of data protection available for young people using digital media platforms. InternetNZ noted that social media platforms gather data on behavioural signals from users, including scroll speed, replay frequency, and typing rhythms.

## 2.2 Experiences shared with us

In this section, we discuss the information and personal experiences that submitters shared with us about the types of harm young New Zealanders experience online. These are organised by the experiences related to content, conduct, contact, and commerce harms. In these descriptions, we link submitters’ experiences of harmful online content and activity to the kinds of effects felt by young people. In each section, we also discuss comments submitters shared with us about how platform design features can contribute to online harm.

### Content harm, prejudice, and social comparison

Submitters highlighted examples of young people facing harm as a result of exposure to content online. They discussed exposure to age-inappropriate content like pornography, violence, social comparison, self-harm, and animal cruelty.

---

<sup>8</sup> Misinformation is information that is false, but not shared with the intent to cause any harm. Disinformation: false or misleading information that is deliberately shared with the intent to cause harm.

<sup>9</sup> Loot boxes are items that contain a randomised reward for players. Gacha mechanics enable players to spend game or real currency to receive a randomised reward.

Netsafe told us that surveys it conducted indicate that nearly half of all young people in New Zealand have encountered harmful content online. Similarly, the Classification Office drew our attention to research it conducted about online content.<sup>10</sup> It found that real-world graphic violence was the most common type of harmful content mentioned by young people.

One submitter, Sarah Higgs, highlighted how children could be exposed to harmful content without seeking it out: “When my son was researching a school project on bees, a simple search of “honey” served up links to adult websites among its genuine search results”. Other submitters also referenced young people being sent harmful content or shown harmful content in targeted advertising.

Stories from submitters demonstrated how platform design features can contribute to content harm. Nadia Maxwell described an experiment she had conducted, setting up accounts on TikTok, Instagram, and Snapchat purportedly as a 13-year-old girl.<sup>11</sup> She reported: “I thought it might take a week for disturbing content to crop up...it took 22 minutes and 15 seconds for the first suicide related video to appear on TikTok.” The direct experiences of young people reflect this. Inspire and Grow Charitable Trust shared an experience from one of the young people involved in its NextGen Leader Academy with us. This young person said, simply: “you don’t have to find porn on social media, it finds you”.

Submitters discussed how exposure to harmful content could negatively affect young people. For example, Mana Mokopuna | Children’s Commissioner said that exposure to online content can negatively affect children’s mental development and worldview. Submitters also described how even content that does not directly depict extremely harmful topics can still lead to harm. In particular, submitters said that exposure to online content can reinforce discriminatory prejudices or bias. For example, the Inclusive Aotearoa Collective Tāhono told us that continued exposure to extremist ideologies can lead young people to hold dehumanising beliefs about other communities. The Australian eSafety Commissioner conducted research into young men’s experiences online and reported that men often reported that algorithms reinforced harmful beliefs about their identities and relationships with others.<sup>12</sup>

Submitters also noted that social media can foster a sense of social competition, leading to both psychological and physical consequences. Mana Mokopuna submitted that exposure to images that promote unattainable beauty standards can result in low self-esteem, body dissatisfaction, and disordered eating. Our Kids Online cited research by the Classification Office and Netsafe. This study found that young people aged between 14 and 17 reported that social media is their most influential source on topics related to body image.<sup>13</sup>

---

<sup>10</sup> [Content that Crosses the Line: Conversations with young people about extremely harmful content online | Classification Office.](#)

<sup>11</sup> The results of this experiment were shared in a New Zealand Herald article: [TikTok shock: ‘Scary’ content pushed to social media feed set up for 13-year-old | NZ Herald.](#)

<sup>12</sup> [Young men online | eSafety Commissioner.](#)

<sup>13</sup> [Digital Reflections: The Online Experience and its Influence on Youth Body Image in Aotearoa | Classification Office.](#)

**Contact harms and sexual violence**

Submitters shared information related to young people being exposed to harmful and unsafe interactions online. In particular, submitters commented on online platforms contributing to sexual violence, grooming, sexual exploitation, and other harmful behaviour.

ECPAT (End Child Prostitution and Trafficking) noted that it conducted interview research in 2025 on child sexual abuse and exploitation, both in-person and online. Its research found that “perpetrators utilised online spaces in which they could be digitally alone and unsupervised with young teenagers.”<sup>14</sup> Other submitters noted that it was not just predators deliberately setting out to sexually exploit young people that can cause harm. Young people representing Dear Em reported that: “We see catfishing used by predators, yes, but also from our own peers who are failing to fully understand their own impacts.”

The Wellington Community Justice Project suggested that features of online platforms can contribute to exposing young people to unsafe interactions. It said that the combination of exposure to digital media that normalises sexual content online, and access to direct messaging, creates an environment where grooming can occur easily.

Submitters said that exposure to sexual violence online can have negative effects on young people, such as psychological, social, and relational consequences. The Light Project described how access to sexual content online can contribute to in-person sexual violence. It reported that young people often use pornography sites as a tool to learn about sex, and argued that this has normalised and contributed to an increase in aggressive forms of sexual activity.

**Conduct harms and deepfakes**

Submitters described examples of online platforms being used to intentionally harm or abuse people, such as through cyberbullying or sextortion.

Cyberbullying was one of the harms most frequently mentioned by submitters. Emily Dyer, a teacher, submitted that she has seen damaging patterns of online behaviour such as secretive friendships and use of social media to humiliate and bully peers. Havelock North Intermediate School argued that social media platforms “allow children to communicate outside adult supervision, and their moderation tools are ineffective at detecting child-to-child harm”. It said it was difficult to detect and take action on bullying between students that occurred online, in comparison to in the classroom.

Submitters highlighted how platform design features contribute to cyberbullying, such as with direct messaging platforms enabling young people to communicate in an unsupervised environment. One anonymous submitter commented that features on Facebook, such as the ability to “unfriend” someone or leave a message marked as being “seen” without responding, can contribute to feelings of social rejection.

Submitters gave numerous stories of cyberbullying causing negative effects on young people’s mental health and social behaviour. A 2023 Netsafe report concluded that

---

<sup>14</sup> “I’m just content to them”: Children living through sexual exploitation in Aotearoa New Zealand | ECPAT, p 30.

cyberbullying does not always result in personal or social harm. However, it cited evidence that cyberbullying can correlate with worse wellbeing.<sup>15</sup>

Submitters also expressed concern about deepfake technology, or “nudify” apps, being used to create false or altered images of child pornography. Dr Cassandra Mudgway cited research finding that 90 to 95 percent of deepfakes online globally are pornography, and disproportionately target women and girls.<sup>16</sup> Laura McClure MP described how deepfake tools and “nudify” apps are easy, fast to use, and have a low threshold to prove consent to use the images provided. She also commented that the production and distribution of sexual deepfake imagery is a legislative grey area.

### **Commerce harms and online advertising**

Submitters said that young people can experience harm online as a result of scams, underage online gambling, and advertising.

Some submitters said that advertising on digital media platforms can promote inappropriate or age-restricted products to young people, such as alcohol, smoking, vaping, or gambling. Save the Children cited research from Deakin University demonstrating that teenagers see an average of six alcohol advertisements and 24 junk food advertisements each day.<sup>17</sup>

Alcohol Healthwatch shared a story from a mother whose daughter had struggled with alcohol addiction, and passed away: “As a mother, I watched my daughter be targeted by an industry that knew her weaknesses better than I did”. Alcohol Healthwatch linked alcohol-related harms to features of digital media platforms. It said that people who consume alcohol more are often targeted more by alcohol-related advertising on digital media. Similarly, it noted that features of e-commerce platforms reduce barriers for young people’s access to alcohol. For example, some e-commerce platforms offer delivery or enable consumers to “buy now, pay later”.

Both international and New Zealand-based research demonstrates that online advertising is associated with alcohol consumption among teenagers. For example, one New Zealand study found that exposure to, and engagement with, alcohol marketing correlated with online purchases and alcohol consumption.<sup>18</sup> A systematic review of 25 studies found that engagement with online alcohol marketing was positively associated with increased consumption and binge-drinking behaviour.<sup>19</sup>

Australia’s National Taskforce for Social Media, Body Image and Eating Disorders also expressed concern that young people are often exposed to advertising for appearance-altering products and procedures. It noted that such advertisements are often in the form of

---

<sup>15</sup> [Cyberbullying in New Zealand | Netsafe](#), pp 15–16.

<sup>16</sup> [2023 State of Deepfakes: Realities, Threats, And Impact | Security Hero](#).

<sup>17</sup> [New research shows kids are targeted with alcohol, gambling and junk food ads online | Institute for Health Transformation](#).

<sup>18</sup> [Alcohol marketing on social media: young people’s exposure, engagement and alcohol-related behaviors | Taylor & Francis Online](#).

<sup>19</sup> [Exposure to Digital Alcohol Marketing and Alcohol Use: A Systematic Review | Journal of Studies on Alcohol and Drugs](#).

partnerships with influencers or online content creators. This can make it harder for young people to distinguish content as advertising, rather than peer-to-peer communication.

### **Benefits of online activity**

Submitters also discussed the benefits that online experiences can bring to young people. For example, submitters highlighted that online platforms may:

- facilitate social connections and relationship development
- provide access to resources and support, including mental health resources
- support individuals to develop a sense of belonging and join communities
- provide access to educational opportunities and resources
- create opportunities for young people to get involved in activism or inform their political views
- enable young people to contact family and friends overseas, such as through using instant messaging features.

Let Me Speak elaborated on how social media platforms in particular can benefit young people socially, enabling them to connect with one another. It commented that social media is “a place of connection, identity, creativity and solidarity. This is especially true for members of marginalised communities – including LGBTQ+ youth, neurodivergent youth and young people with disabilities or in rural or isolated areas”. The Disabled Persons Assembly NZ echoed this point. It told us that access to the internet removes barriers and enables disabled people to participate in society “more easily and quickly”.

The Stratford District Youth Council also told us that access to social media is important for supporting young people’s business enterprises and access to jobs. It commented: “Not only is social media a place for connections, it is also a place where enterprising young Kiwis can thrive—from students searching for work, doing odd jobs or babysitting, to young people promoting media-based businesses.” The Stratford District Youth Council said that access to social media platforms enables young people to develop digital literacy skills, which can be important for the workplace.

Professor Emma Rich cited research based in the United Kingdom on digital health technologies.<sup>20</sup> The study surveyed young people and found that 70 percent of them used digital health technologies, and 55 percent of them used smartphones, to manage or learn about their health.

## **2.3 Research and understanding of online harm**

Submitters noted that there is little research into online harm in the New Zealand context. Many submitters said it would be beneficial to have more New Zealand-based research to monitor and gain further understanding of online harm. Other submitters highlighted the limitations of existing research. For example, Netsafe reported that:

Research in this area is often contradictory or inconclusive, and it is difficult to establish causation rather than correlation. We are also aware of the ethical

---

<sup>20</sup> [Digital Health Generation Report | Professor Emma Rich.](#)

constraints on conducting research with young people but it is important that adult centred research is not used in place of the youth experience. If the evidence base is incomplete or unclear, this should trigger further research.

Some submitters offered cautious views as to whether the evidence base proves that digital media *causes* or *correlates* with harm. It can be difficult to accurately measure the effects of digital media. Researchers must consider bi-directional effects, such as whether social media use contributes to poor mental health, or whether young people with poor mental health are more likely to use social media. Effects may also be the result of environmental or unrelated factors.

Other submitters criticised this point of view. Dr Samantha Marsh maintains that current research into the effects of digital media does demonstrate causation. She cited an experiment in which reducing smartphone use showed improvements in depression symptoms, stress, sleep quality, and wellbeing.<sup>21</sup> The Australian National Taskforce for Social Media, Body Image and Eating Disorders also cited a meta-analysis that demonstrated that viewing online content related to beauty ideals can be harmful to viewers' body image, mood, and eating-disorder symptoms.<sup>22</sup>

Submitters on both sides of this argument emphasised the importance of relying on high-quality systematic reviews and meta-analyses rather than independent studies to inform policy responses in this area.<sup>23</sup>

Further links to resources and research about online harm experienced by young New Zealanders are included in Appendix C of this report (see p 45).

## 2.3 Our response and reflections

We would like to thank everyone who made a submission on the inquiry. We appreciated submitters' thoughtful engagement with us and insightful discussions during the hearings. In particular, we thank all the children and young people who submitted for their courage in sharing their personal experiences with us. Overall, we were greatly impressed with the quality of submissions and the range of evidence, experiences, stories, and opinions.

The strong impression from submitters is that online harm in New Zealand is widespread and deeply felt by young people. We acknowledge the complexity in proving direct causation between digital media and harmful effects on young people. However, we conclude that we have received sufficient evidence to say that online harm is a public health issue that requires collective attention from Government, businesses, online platforms, and civil society.

While our inquiry focuses on online harm, we recognise that online activity can have positive effects, such as on young people's learning, social development, and sense of community.

---

<sup>21</sup> [Smartphone screen time reduction improves mental health: a randomized controlled trial | PubMed.](#)

<sup>22</sup> [Social media, body image, and the question of causation: Meta-analyses of experimental and longitudinal evidence | ScienceDirect.](#)

<sup>23</sup> Systematic reviews are a research method used to synthesise research available on a certain topic. A meta-analysis is a statistical research method that uses data from multiple independent studies to determine overall trends or conclusions.



In our terms of reference, we noted we would also consider the benefits that online activity may offer to young people, and the extent to which these benefits are realised. We recognise that in designing potential solutions to address online harm, the prevalence of both the harm and benefits provided by online activities needs to be considered.

## **3 Approaches to addressing online harm in New Zealand**

In this chapter, we discuss New Zealand's current legislative framework for addressing online harm, and the current approaches that online platforms, parents, educators, and civil society are taking to prevent online harm. In each section, we provide an overview of current arrangements and then summarise main themes from submitters related to the advantages and limitations of these approaches.

Many submitters referred to legislative and regulatory settings in New Zealand that relate to online content or activity. Multiple submitters commented that the overall regulatory approach seemed fragmented. Submitters expressed concerns about gaps in the legislation for dealing with harms caused by emerging technology, like AI.

Some submitters were concerned that New Zealand does not have a framework to assess the harms posed by the design of platforms. The design of online platforms and algorithms plays an important role in the kinds of experiences that young people have online.

Parents and teachers who submitted often felt that they do not have the skill, knowledge, or resources to prevent and respond to online harm. There was a general feeling that education and other non-regulatory responses are inconsistently applied and available.

### **3.1 Current legislative and regulatory settings**

New Zealand has multiple pieces of legislation that relate to online content regulation. However, no specific legislation regulates online platforms for user safety. Online harms are also indirectly addressed in legislation related to privacy, security, crimes, and human rights. For example, the New Zealand Bill of Rights Act 1990 affirms fundamental human rights and freedoms in New Zealand. These rights also apply in online contexts.

This section first provides an overview of some of the key pieces of legislation in New Zealand that aim to help protect people from online harm. We then summarise key themes from submitters related to this topic.

#### **Legislation related to content moderation or online conduct**

The Harmful Digital Communications Act 2015 aims to prevent harm caused to individuals by digital communications and provide victims with an avenue for redress. It empowers Netsafe, an independent non-profit organisation, to operate as the approved body to investigate complaints into harmful digital communications. The Act also introduced new offences, making it illegal to post an intimate visual recording of someone or post digital communications with the intention to cause harm.

The Harmful Digital Communications Act also set up a "safe harbour" process that protects online platforms from legal responsibility for content that other people post on their platforms. Hosts of online platforms can normally be held legally responsible for the content on their

platform, even if they did not create or post it. If content hosts follow the “safe harbour” process as outlined in the Act, they can no longer be held liable for such content.

The Films, Videos, and Publications Classification Act 1993 regulates the classification of publications, including films, television shows, and online content. The Act established the Classification Office, an independent Crown entity focused on keeping New Zealanders safe from content harms. The Classification Office has a mandate to prevent exposure to harmful content, while upholding the right to freedom of expression and empowering New Zealanders to make informed choices about content they engage with. It is responsible for classifying publications that may need to be banned—such as objectionable material, and publications that may need to be restricted. For example, it can issue restricted age-ratings for films. The Classification Office also monitors and approves specific commercial video streaming services to self-rate the content they provide to New Zealanders. It conducts research and produces educational resources related to media literacy.

There is no specific “safe harbour” provision in the Films, Videos, and Publications Classification Act.

The Films, Videos, and Publications Classification Act was amended in 2021.<sup>24</sup> Amendments included making it illegal to livestream objectionable material and enabling the Classification Office to issue take-down notices for objectionable material online. Amendments also introduced new provisions for the Chief Censor to issue interim decisions to respond to extremely harmful material quickly.

Other relevant pieces of legislation include the Broadcasting Act 1989 and the Unsolicited Electronic Messages Act 2007. The Broadcasting Act established the broadcasting standards regime and complaints process, and regulates advertising. The Unsolicited Electronic Messages Act makes it illegal to send unsolicited commercial electronic messages.

In 2022, Netsafe and NZTech launched the Aotearoa New Zealand Code of Practice for Online Safety and Harms.<sup>25</sup> The code sets out commitments by signatories to enhance online safety and reduce harmful content online. It has been signed by companies such as Meta, Google, TikTok, Twitch, and X. The code is a voluntary agreement.

New Zealand also has organisations responsible for investigating complaints regarding some forms of digital media. The New Zealand Media Council investigates complaints related to media, including about the accuracy, fairness, and balance of news media. It can investigate complaints related to some forms of online content. This includes content produced by New Zealand newspapers, magazines, and certain broadcasters. Similarly, the Advertising Standards Authority investigates complaints about advertisements that are not legal, decent, or honest. This includes advertising online and on social media.

---

<sup>24</sup> Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Act 2021 | New Zealand Legislation.

<sup>25</sup> Aotearoa New Zealand Code of Practice for Online Safety and Harms.

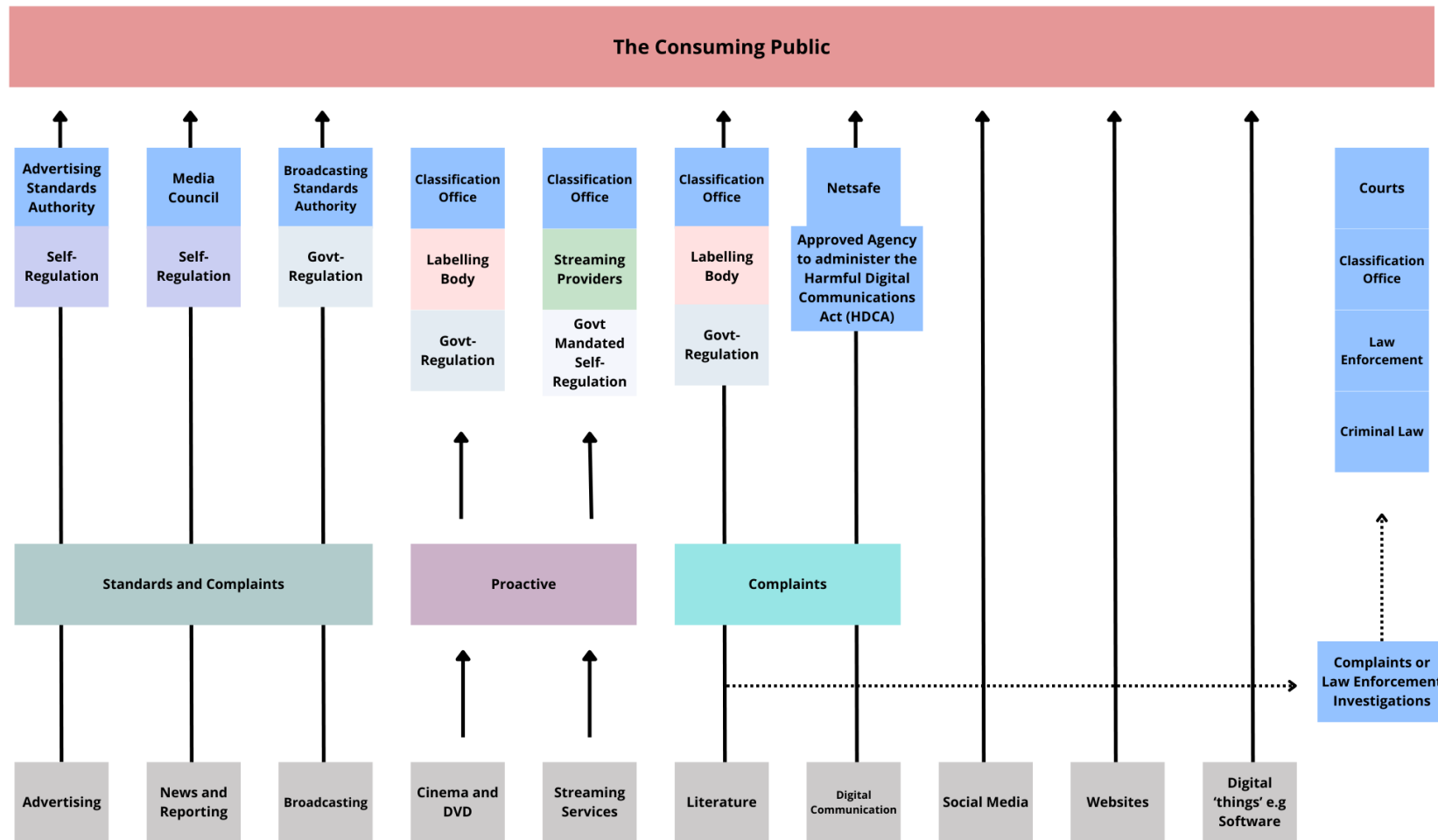


Figure 2: New Zealand legislation related to online content and activities

## **Challenges regulating online harm in New Zealand**

Submitters frequently described legislation as “fragmented” and said that this is a barrier to effectively addressing online harm. The National Council of Women of New Zealand said: “In general, our legislation deals with individual pieces of content and has a fractured mix of media regulatory bodies, none of which have modern regulatory powers to influence system-wide controls and levers.”

Netsafe said that as well as online content being regulated through various pieces of legislation, multiple government departments hold responsibilities related to online harm. It commented that while the Department of Internal Affairs holds policy responsibility for digital safety, the work of other government agencies often intersects. For example, the Ministry of Business, Innovation and Employment is responsible for scams policy, and the Ministry of Health is responsible for policy related to mental health and wellbeing.

Submitters expressed concern that no clear, single authority is tasked with coordinating the response to online harm. Several commented that it could be beneficial to introduce a national regulator responsible for online safety. They said this could help make it clear where people should go when they encounter harm.

Another challenge identified by submitters is that it is difficult for regulatory or policy responses to keep up with the rapid pace of technological development. Submitters felt that New Zealand’s legislation is not fit for purpose or able to respond to emerging challenges, like developments in AI. The National Collective of Independent Women’s Refuges | Ngā Whare Whakaruruhau o Aotearoa said there is a “lag” between technological developments and the ability of the justice sector to understand and respond to new forms of digital illegal activity.

Submitters worried that the combination of a fragmented regulatory landscape and the fast-paced development of technology creates gaps that mean some online harms are not being effectively addressed. Retail NZ recalled that Netsafe received 28,468 reports of online harm in 2024. However, data from the Ministry of Justice shows that only 71 people were convicted under the Harmful Digital Communications Act in that year.

## **Addressing sexual violence online**

Submitters expressed deep concern that New Zealand legislation does not effectively protect young people from sexual violence online. In particular, submitters said that the creation of sexual deepfake imagery is not effectively addressed. The Crimes Act 1961 and the Harmful Digital Communications Act both address the non-consensual recording and sharing of intimate material. However, both Laura McClure and Dr Cassandra Mudgway pointed out that these laws do not cover the creation or distribution of altered or false imagery, like deepfakes.

Deepfake pornography would be covered under the Films, Videos, and Publications Classification Act if it meets the criteria to be classified as an “objectionable” publication. The Act defines publications as objectionable if they describe, depict, express, 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. Sexual images of children, including altered images, are considered objectionable. It is illegal to create, possess, or distribute any objectionable

publication. However, the technology used to create this type of content is not illegal or subject to regulation in New Zealand.

## **Algorithms and platform design**

Submitters noted that there are no mechanisms to regulate the design of online platforms or algorithms in New Zealand.

Recommendation algorithms are often used on social media platforms to personalise, recommend, and sort the content that a user sees. These algorithms often sort and present content that aligns with its prediction of a user's interests, based on factors like behavioural signals, past engagement, or demographics. Content popularity or relevance may also influence algorithms' decision-making. Often users are aware of algorithms on social media but do not fully understand how they operate or affect their experiences.

In its submission, InternetNZ highlighted that there are no current settings to address harm caused or amplified by platforms' algorithm design. It commented that there are technical limitations to the transparency of platform algorithms. It said that researchers are not often given access to raw algorithms, meaning that independent research often relies on partial data that may misrepresent actual algorithmic activity.

We discuss international efforts to address algorithm transparency and the challenges involved later in the report (*see pp 35–36*).

## **3.2 Roles and responsibilities of online platforms**

The infrastructure and features of online platforms can contribute to or mitigate harms felt by young people, depending on the design choices that companies make. Submitters were concerned that platforms' design choices often prioritise their own commercial goals ahead of users' safety. Most digital media platforms depend on advertising revenue; this fact influences the kind of design and policy choices that these companies make.<sup>26</sup> In 2024, Meta reported that advertising was 98 percent of its total revenue. Similarly, advertising comprised 77 percent of TikTok's total revenue and 68 percent of X's total revenue in 2024.<sup>27</sup> The longer users spend on a platform, the more likely they are to be exposed to advertising.

We received submissions from online platforms and technology companies, Google, Meta, and TikTok.<sup>28</sup> These companies provided information to us about their current protective mechanisms and online safety measures.

There is tension between the information that online platforms provided us and the overall sentiment from submitters. Online platforms assured us that they had extensive mechanisms in place to keep young people safe online. In contrast, submitters considered that platforms could do more to prevent and respond to harm. These differences may arise due to low

---

<sup>26</sup> [Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media | Research Gate](#).

<sup>27</sup> [Social media, misinformation and harmful algorithms | United Kingdom House of Commons](#).

<sup>28</sup> Google owns YouTube and Meta owns Facebook, Messenger, Instagram, and WhatsApp.

awareness of platforms' safety features, different expectations of the level of action required, or limited effectiveness of online platforms' efforts.

### **Online platforms' efforts to improve online safety**

Google, Meta, and TikTok all agreed that they have a responsibility to create and maintain a safe online environment for young people. Each platform said they have online safety mechanisms, including age-appropriate products, tools, and policies. All three of these companies' online platforms have minimum age restrictions, requiring users to be over 13 years old to create an account.

Both Google and Meta said that they have specific accounts and user experiences designed to protect younger users. YouTube Kids is a filtered version of YouTube designed to show only content appropriate for children. Similarly, Meta offers Teen Accounts on Instagram, Facebook, and Messenger. These are account types designed for 13- to 17-year-olds that are set to more protective settings that require parental permission to change. Google, Meta, and TikTok each also described their parental control features that enable parents to oversee the social media use of children under the age of 16.

The online platforms each said they have community guidelines about the kinds of content and activities allowed on their platforms. All three companies highlighted their efforts to moderate and remove online content that breaches these standards. For example, Meta said it removed 5.1 million pieces of bullying and harassment content globally in the first quarter of 2025. Similarly, it took action on 6.8 million pieces of content on Facebook and 9.9 million pieces of content on Instagram related to suicide and self-harm in the first quarter of 2025. TikTok said it had removed more than 1.3 million videos in New Zealand since 2023. Platforms emphasised that they take proactive steps to address extremely harmful material, such as child sexual abuse material.

Google said it had updated its recommendation algorithms to limit young people's exposure to harmful content. This included content related to negative social comparison and real-world aggression. Similarly, Meta said that while it does not disallow content related to mental health, self-harm, and eating disorders, its recommendation systems hide this kind of content to make it harder to find. It said that if users search for terms related to suicide or eating disorders, they will be directed to support resources.

Meta said it offers some transparency of its algorithms, such as platform features that enable a user to find more information on why they are seeing a particular piece of content or an advertisement. Meta has system cards explaining how its AI recommendation systems on Facebook and Instagram work at a high level.<sup>29</sup> Meta also offers access to its content library and Application Programming Interface (API) to researchers from qualified institutions.<sup>30</sup> TikTok provides access to its commercial content library and API in Europe and the United States. However, we understand that audit analysis has found the data provided by TikTok to be incomplete.<sup>31</sup>

---

<sup>29</sup> [Introducing 22 system cards that explain how AI powers experiences on Facebook and Instagram | Meta.](#)

<sup>30</sup> [Content Library and API | Meta.](#)

<sup>31</sup> [Supporting independent research | TikTok.](#)

Submitters representing gaming industry companies also highlighted their efforts to improve online safety. The International Games and Entertainment Association said it provides mechanisms to limit age-inappropriate content, set limits on how long children can play, manage spending, and monitor who children can communicate with online.



	YouTube	Meta	TikTok
<b>Age appropriate products and settings</b>	<ul style="list-style-type: none"> <li>• YouTube kids</li> <li>• Supervised experiences (for children under 13)</li> <li>• Voluntary Teen supervision option for 13 - 17-year-olds</li> </ul>	<ul style="list-style-type: none"> <li>• Teen accounts on Instagram, Facebook, and Messenger</li> </ul>	<ul style="list-style-type: none"> <li>• Did not specify a specific product but highlighted that they have strong age enforcement systems (age 13)</li> <li>• More restrictions on accounts registered to users under 16</li> </ul>
<b>Tools and settings examples</b>	<ul style="list-style-type: none"> <li>• Autoplay is turned off by default on YouTube Kids</li> <li>• In Supervised Experiences, a parent can completely disable autoplay</li> <li>• 'Take a Break' reminders</li> </ul>	<ul style="list-style-type: none"> <li>• 'Restrict' tools in Instagram</li> <li>• Bullying and harassment warnings on Facebook and Instagram to accounts with potentially bullying or harassing comments</li> <li>• Parental control to set up screen time and control child's accounts</li> </ul>	<ul style="list-style-type: none"> <li>• Family pairing tools offers a range of privacy and safety settings</li> <li>• Parental control to set up screen time and control child's accounts</li> </ul>
<b>Approaches to address online harm</b>	<ul style="list-style-type: none"> <li>• No targeted ads for users under 18</li> <li>• Content prohibition on specific content (food, beverages, religion, politics) in accounts restricted to younger users under 16</li> </ul>	<ul style="list-style-type: none"> <li>• Removal of potentially harmful content e.g. self-harm and suicide</li> <li>• Offering tips and links to support services e.g. when a user repeatedly searches for eating disorder related content</li> </ul>	<ul style="list-style-type: none"> <li>• Make content ineligible for the For You feed when the content does not meet TikTok's recommendation standards.</li> <li>• Restrict content that is not suitable for younger audiences</li> </ul>
<b>Partnerships</b>	<ul style="list-style-type: none"> <li>• YouTube's Youth and Families Advisory Committee - a collection of independent experts support Google's products, policies, and services.</li> <li>• Squiz Kids; the partnership rolled out "Newshounds", which is a resource for teachers, children and their parents in NZ.</li> </ul>	<ul style="list-style-type: none"> <li>• Netsafe New Zealand</li> <li>• Youthline</li> <li>• Safeguarding Children New Zealand</li> </ul>	<ul style="list-style-type: none"> <li>• Regional Safety Advisory Councils - Council members are made up of experts in youth safety, free expression, hate speech, and other safety topics</li> <li>• Netsafe New Zealand</li> </ul>

Figure 3: *Online platforms' approaches to online safety for young people.*

## Limitations of online platforms' self-regulation

Many submitters were of the opinion that online platforms should do more to address online harm. For example, submitters said they should improve their operational policies and online safety mechanisms. Common recommendations from submitters were that platforms should:

- develop clear guidelines and policies to address cyberbullying, racism, and other harmful content
- improve content moderation and reporting mechanisms
- ensure safety and privacy mechanisms are easy for users to access
- enforce current age-restriction and verification systems on social media platforms
- strengthen advertising restrictions and age-appropriate settings for children
- publish transparency reports about their algorithms, content moderation policies, and risk assessments.

Save the Children drew our attention to a survey of young New Zealanders it conducted alongside Netsafe. Results showed that 75 percent of participants recommended having more control over advertisements and content as an action that would improve their online experiences.<sup>32</sup>

Submitters said that online platforms should prioritise user safety at the forefront of platform development, rather than introducing online safety mechanisms in retrospect. Some submitters said that regulatory measures should be introduced to mandate certain online safety standards or design requirements that platforms must meet. These submitters felt there are limitations to online platforms being left to self-regulate and set their own policies, community standards, and terms and conditions.

The extent to which online platforms choose to self-regulate, and the effectiveness of these measures, is limited by platforms' business choices and commercial incentives. Submitters highlighted a key tension in this area. Often, features that submitters said contribute to or exacerbate online harm are key to platforms' business models. For example, recommendation algorithms are used to personalise social media feeds, which enables targeted advertising or promotion of specific content. Submitters expressed concern that recommendation algorithms may encourage addictive use of social media or drive harmful content towards young people. This suggests there is a conflict between the business interests of digital media platforms and their ability to effectively reduce online harm.

## 3.3 Roles and responsibilities of parents, educators, and civil society

There are no legal obligations on parents to ensure that children are protected from online harm. However, many submitters discussed the role parents, caregivers, family, and communities have in protecting young people. Some submitters said that parents should monitor children's online activity and ensure protections are in place. Meta and TikTok also expressed agreement that parents and guardians have a key role in keeping young people safe online. TikTok cited survey research conducted by Talbot Mills that found that 81

<sup>32</sup> [Children and youth online safety in Aotearoa New Zealand | Save the Children.](#)

percent of respondents believed that parents should decide when young people can start using social media.<sup>33</sup>

Submitters often discussed the importance of having conversations with young people about digital literacy in this context. Save the Children said that children have high rates of digital media consumption, claiming that “the highest users of YouTube in New Zealand are under five”.<sup>34</sup> It discussed the importance of having conversations about digital media with young children about when they use digital media and why they choose to use it.

At the same time, many submitters also felt that young people, parents, and educators do not have access to enough resources or training in digital literacy. Our Kids Online referenced the results of a survey it conducted into online safety. Of the 4,671 parents and caregivers it surveyed, 93 percent were totally unaware or only slightly aware of solutions to minimise online harms to young people.<sup>35</sup> Some submitters suggested that there should be public education campaigns on online safety, similar to initiatives that have been carried out for smoke-free and road safety campaigns.

Both Netsafe and the Classification Office conduct research and provide resources on online safety in New Zealand. However, some submitters indicated that they did not know where to go to find digital literacy resources. Submitters also commented that there is a lack of educational resources available in te reo Māori. Links to further research on online safety in New Zealand and helpful resources for young people and families are included in Appendix C of this report (*see p 45*).

Other submitters questioned the ability of educational measures to mitigate online harm. Professor Emma Rich drew our attention to research on digital health technologies in the United Kingdom.<sup>36</sup> She commented that content on social media can contribute to low self-esteem and increase anxiety about body image, even when young people understand that such content is not real or representative. Professor Rich stated that even when young people demonstrate media literacy skills, such as recognising when images on social media have been edited, “this awareness did not stop them from internalising unrealistic ideals or feeling inadequate”.

Submitters also discussed how parents, educators, and community members are often the first people that young people approach to seek support. We heard that submitters feel that there are inadequate pathways to report online harm or seek support. Aotearoa Free From Stalking commented that schools, parents, and mental health services may not have specific knowledge of the online environment needed to offer well-informed support. It told us that “This lack of systematic support compounds the harm, leaving young Kiwis feeling isolated with their distress.” Teachers shared stories with us of children approaching them for help and acknowledged that they are not always trained to provide the level of mental health support required.

---

<sup>33</sup> [Kiwis trust parents to decide when young people can start using social media | TikTok](#).

<sup>34</sup> Recent research conducted by NZ On Air found that 69 percent of New Zealand children aged 2–14 use YouTube or YouTube Kids every day. [Research highlights need for a new approach to serving children local media | NZ On Air](#).

<sup>35</sup> [Online Safety Awareness Survey | Our Kids Online](#).

<sup>36</sup> [Digital Health Generation Report | Professor Emma Rich](#).

Our Kids Online also advocated for the development of online safety technology that could support parents and caregivers to monitor or manage their children's online activity. It suggested that each households have two Wi-Fi routers, one of which has a child-safety filter on it to restrict access to certain content or online platforms. Similarly, it advocated for specific SIM cards for under 18-year-olds that have content filters. We note that similar technologies are available for use internationally.

## **3.4 Our response and reflections**

### **Limitations of current legislation in New Zealand**

We believe there are limitations to how effective current laws and regulatory approaches can be in responding to an online context. Online platforms are not liable for user-generated content hosted on their platforms under the “safe harbour” process in the Films, Videos, and Publications Classification Act and Harmful Digital Communications Act. We agree with submitters' concerns that the current legislative landscape and areas of responsibility are fragmented. Submitters generally supported the idea of having a national regulator to oversee the system, ensure platforms are properly regulated, and enforce compliance.

We understand that the fast development of technology creates new challenges that need to be responded to quickly to avoid regulatory gaps where harm can happen. Emerging technologies, such as generative AI and deepfake technology, illustrate a need for regulatory responses to be agile to respond to new risks.

### **Regulating online platform design and safety features**

We observed a disconnect between submissions presented by online platforms and those from the general public. Online platforms presented the range of online safety features they have available to protect young people. We encourage this work and are glad to see that online platforms already have a range of safety tools. However, we agree with submissions from the New Zealand public that this work needs to go further.

We consider that there is a level of conflict between the business models of social media platforms and the need to most effectively shield young people from harm. We consider that social media platforms have a commercial incentive to design their platforms to be addictive and stimulating for young people. However, these features may contribute to psychological and behavioural harm. We also understand that there are commercial and reputational reasons why platforms may not wish to highlight their own role in creating online environments where young people face harm.

We understand that there are both technical and privacy concerns related to providing algorithmic transparency. We explore international efforts to improve algorithmic transparency later in this report (see *pp 35–36*). We also intend to investigate this issue further in our final report.

### **Resourcing parents, educators, and young people with digital literacy skills**

We believe parents, caregivers, and adults have a strong role to play in protecting young people from online harm and teaching them how to safely navigate online environments.

However, we recognise that this can be a challenging role for parents and caregivers. We are of the view that parents do hold the primary responsibility for their own children.

We acknowledge submitters' concerns that there are insufficient resources available to help teach both young people and parents about digital literacy. This is made more complex as parents themselves vary widely in their level of digital literacy. While some parents may have grown up with internet access and have a lot of knowledge about the digital environment, this is not the case for all caregivers. Similarly, internet connectivity and access to digital products and services varies across New Zealand. The affordability of internet connectivity and digital services may also limit access for some people. Rural areas are more likely to report connectivity problems, such as limited bandwidth or unreliable coverage.<sup>37</sup> These factors can make it difficult for parents to communicate effectively with young people about their digital experiences.

---

<sup>37</sup> [Rural Users Digital Connectivity Experiences | Ministry for Primary Industries.](#)

## 4 International experiences

### 4.1 Summary of experiences in similar jurisdictions

In recent years, similar jurisdictions have taken steps to introduce legislation or other approaches to address the risk of online harm. This section summarises key pieces of legislation in Australia, the European Union, Ireland, and the United Kingdom. While approaches vary between countries, these frameworks impose greater responsibilities on platforms to proactively address and be held accountable for online harm.

There are common challenges in introducing legislation that governs online safety. For example, it is difficult to enforce online safety mechanisms across different jurisdictions or to determine legal liability for content shared online. There are also different approaches to striking a balance between regulating to reduce harm and protecting freedom of expression and privacy rights.

Different countries also have different approaches to how internet service providers and online platforms are held liable for providing access or hosting harmful content created by third parties.

#### Australia

In 2021, Australia enacted the Online Safety Act 2021.<sup>38</sup> The Act established an eSafety Commissioner responsible for regulating online platforms, establishing basic online safety mechanisms, and issuing removal notices for online content.<sup>39</sup> The eSafety Commissioner can issue notices that require:

- online services to take all reasonable steps to remove illegal content from their platform
- internet search engines to stop providing links that enable Australian users to access illegal material
- internet service providers to block access to material that promotes or depicts abhorrent violent material if the Commissioner is satisfied that the material is likely to cause significant harm to the Australia community.

Failure to comply with notices issued by the Commissioner may result in a range of enforcement measures, from formal warnings to penalties.

The eSafety Commissioner also provides advice and resources for educators, parents, and young people, including an eSafety Toolkit developed for schools.<sup>40</sup> Australia's Privacy Act 1988 also regulates how government agencies and certain organisations treat personal information online.<sup>41</sup>

---

<sup>38</sup> [Online Safety Act 2021 | Federal Register of Legislation.](#)

<sup>39</sup> [Online safety | eSafety Commissioner.](#)

<sup>40</sup> [Toolkit for Schools | eSafety Commissioner.](#)

<sup>41</sup> [The Privacy Act 1988 | Australian Government.](#)

An independent statutory review of the Online Safety Act found that the Act is most effective at responding to online harm, helping people after they experience harm.<sup>42</sup> For example, the Act enables people to make a complaint to the eSafety Commissioner, who can issue a notice to have harmful content removed. A key recommendation of the review was that Australia also require online platforms to take reasonable steps to prevent harm from occurring. In response to this finding, the Australian Government has committed to introducing a “Digital Duty of Care” on online services to help prevent serious online harm. Public consultation to inform the approach for the proposed duty of care was recently open: between 14 November and 7 December 2025.<sup>43</sup>

Australia has also introduced social media age restrictions. These are discussed in further detail later in the report (see p 35).

In September 2025, the eSafety Commissioner took enforcement action against a company responsible for providing “nudify” and deepfake tools that were used to create AI-generated sexual imagery of Australia school children. On 2 September 2025, the Australian Government announced its intention to restrict access to “nudify” apps and undetectable online stalking tools.<sup>44</sup>

### **United Kingdom**

In the United Kingdom, the Online Safety Act 2023 requires technology companies to protect users’ safety online.<sup>45</sup> The strongest protections in the Act have been designed to ensure children’s safety. The Act introduced new offences, making it illegal for people to conduct certain activities online, including encouraging or assisting serious self-harm, sending threatening communications, and engaging in intimate image abuse. It also empowered Ofcom as an independent regulator for online safety.<sup>46</sup>

The Act introduced duties of care on online platforms and internet search services that, among others, require them to:

- take measures to prevent people from encountering illegal content
- mitigate and manage the risk of harm to children and prevent children from encountering harmful content, such as pornography, violent material, self-harm, and eating disorder promotion
- complete risk assessments related to illegal content and children’s access to content and services.

If Ofcom is satisfied that a service has failed to comply with its duties, it can issue a notice requiring services to comply to remedy the breach. It can also require services to pay penalties.

---

<sup>42</sup> [Report of the Online Safety Act Review released | Ministers for the Department of Infrastructure.](#)

<sup>43</sup> [Digital Duty of Care | Australian Government.](#)

<sup>44</sup> [Taking a stand against abusive technology | Ministers for the Department of Infrastructure.](#)

<sup>45</sup> [Online Safety Act | GOV.UK.](#)

<sup>46</sup> [Ofcom.](#)

The Act does not require online services to moderate content that is uploaded in private communications, such as private direct messages.

Much of the criticism appears to relate to concerns that restrictions are affecting users over the age of 18. This could be happening because:

- regulated platforms might over-block/censor content in order to meet compliance requirements, particularly those that host user-generated content and permit adult content within their policies.
- platforms' age verification methods are ineffective.

The United Kingdom's Free Speech Union expressed its view of the limitations of online regulation in the United Kingdom. It told us that downloads of VPNs have increased in the United Kingdom, following the introduction of the Online Safety Act.<sup>47</sup> The Free Speech Union said that the United Kingdom Government has announced that it is looking "very closely" into the use of VPNs.<sup>48</sup>

## **Ireland**

Ireland's Online Safety Framework comprises relevant European Union legislation and its Online Safety and Media Regulation Act 2022.<sup>49</sup> The Act established a media commission, Coimisiún na Meán, led by an Online Safety Commissioner.<sup>50</sup> The Commissioner is responsible for issuing an online safety code that sets out actions that online platforms must take to protect the public from harmful content. Coimisiún na Meán is also empowered to issue notices to end non-compliance, to seek to block access to certain online services, and to issue notices to limit harmful online content on designated online services.

Coimisiún na Meán is the nationally empowered Digital Service Coordinator for Ireland, acting under the European Digital Services Act 2022.

## **European Union**

The European Union (EU) has also introduced multiple measures that relate to online safety or activity. The Digital Services Act 2022 requires online platforms to implement safety measures to protect young people and to remove illegal content.<sup>51</sup> The Act requires that:

- online platforms implement measures to ensure the safety of minors, including tools for age verification and parental controls
- very large online platforms identify and take steps to mitigate potential risks to minors<sup>52</sup>
- online platforms restrict advertising based on the profiling of users who are minors
- online platforms offer tools to help minors report abuse or obtain support.

---

<sup>47</sup> [VPNs top App Store charts as UK age verification kicks in | BBC.](#)

<sup>48</sup> [Could VPNs be banned? UK government to look "very closely" into their usage following spike after age verification row | TechRadar.](#)

<sup>49</sup> [Online Safety and Media Regulation Act 2022 | Government of Ireland.](#)

<sup>50</sup> [Ireland's media regulator | Coimisiún na Meán.](#)

<sup>51</sup> [The Digital Services Act package | European Commission.](#)

<sup>52</sup> Very large online platforms are those with more than 45 million average monthly users in the EU.



The Act exempts internet service providers from liability for information transmitted, accessed, or stored across their services, as long as certain conditions are met.

At the same time as it introduced the Digital Services Act, the EU enacted the Digital Markets Act, which aims to establish a level playing field for businesses online.

The Audiovisual Media Services Directive also aims to protect young people in the EU from online harm. The directive requires video-sharing platforms and audiovisual services to protect children from harmful material and advertisements.<sup>53</sup>

The General Data Protection Regulation also governs how the personal data of EU residents can be processed and used, including online data.<sup>54</sup>

## **Brazil**

Although not necessarily a comparable legal jurisdiction, we were also interested in what measures Brazil has introduced to address online harm. The Civil Framework for the Internet (*Lei 12.965 2014*) sets out the rights and obligations for usage of the internet in Brazil. There is no dedicated internet regulator. However, courts are empowered to issue and enforce take-down notices for content which is deemed to be unlawful. The framework made online platforms liable for the removal of child sexual abuse material and nonconsensual sharing of intimate images, as well as other unlawful or harmful content, if a judicial take-down notice is issued.

In June 2025, the Brazilian Supreme Court ruled that the framework was partially unconstitutional. Following the Supreme Court decision, online platforms were made liable for the removal of any infringing content if notified of its presence, even if a take-down notice had not been issued. Only content considered as slander, libel, or defamation continues to require a take-down notice for online platforms to be made liable.

---

<sup>53</sup> [Audiovisual Media Services Directive | European Union.](#)

<sup>54</sup> [General Data Protection Regulation | European Union.](#)

	Legislation	Empowered regulatory body/bodies	Regulatory model	Scope	Enforcement	Recent developments
AUSTRALIA	<p>Online Safety Act 2021</p> <ul style="list-style-type: none"> <li>Empowers the eSafety Commissioner (eSafety) to regulate online platforms.</li> </ul>	<ul style="list-style-type: none"> <li>eSafety is responsible for the implementation and enforcement of the Online Safety Act.</li> <li>eSafety has transparency and information request powers.</li> <li>Enforces and monitors industry compliance with the codes and standards.</li> </ul>	<p>The Australian Government sets the Basic Online Safety Expectations for online service providers to ensure safe use of their platforms.</p> <p>Industry Codes &amp; Standards regulate the most harmful online content e.g., sexual abuse of children, and terrorist content.</p> <p>Industry Codes prevent children &amp; young people from access or exposure to age-inappropriate material e.g., pornography.</p> <p>Voluntary Online Dating Code is an industry code that aims to improve safety on dating services. It has no legislative powers.</p>	<p>Electronic carriage services i.e., listed services that enable end-users to access the internet.</p> <p>It includes services that enable users to communicate by email, instant messaging, SMS (text messages), MMS (text, images, videos, audio), chat, and online games.</p> <p>This covers:</p> <ul style="list-style-type: none"> <li>Social media platforms</li> <li>Internet Service Providers</li> <li>App distribution services (e.g., Apple Store)</li> <li>Search engines</li> <li>On-demand program services</li> </ul>	<ul style="list-style-type: none"> <li>The Basic Online Safety Expectations are backed by civil penalties for online service providers that do not meet their reporting obligations.</li> <li>Can issue take down notices for illegal content.</li> </ul>	<ul style="list-style-type: none"> <li>Statutorily reviewed from 2023-2024.</li> <li>Amended in 2024 to include social media age restrictions.</li> <li>From 10 December 2025, age-restricted social media platforms will be required to take reasonable steps to prevent Australians under the age of 16 from creating or keeping an account.</li> <li>The age restriction is expected to apply to Facebook, Instagram, Snapchat, TikTok, X, and YouTube.</li> </ul>
UNITED KINGDOM	<p>Online Safety Act 2023 (OSA)</p> <ul style="list-style-type: none"> <li>Makes social media companies and search services more responsible for users' safety on their platforms.</li> <li>The protection of children is prioritised over adults.</li> <li>Protects users' rights to freedom of expression and privacy and ensures transparency and accountability.</li> </ul>	<ul style="list-style-type: none"> <li>Office of Communication (Ofcom) is the regulator for UK communications services.</li> <li>Ofcom is empowered to assess and enforce providers' compliance with the framework.</li> </ul>	<p>Platforms/services are required to identify, mitigate, and manage the risks of harm from illegal content and activity, and content and activity that is harmful to children.</p> <p>The obligations are set in the online safety rules.</p>	<p>"User-to-user services" that allow people to generate and share content for other people to see.</p> <p>Includes:</p> <ul style="list-style-type: none"> <li>Social media</li> <li>Private messaging</li> <li>Dating services</li> <li>File and audio-sharing</li> <li>Cloud-storage and sharing</li> <li>Gaming services</li> <li>Search engines</li> <li>Services hosting pornographic content.</li> </ul>	<ul style="list-style-type: none"> <li>Ofcom can issue fines to services for failing to comply with their duties – these powers are not limited to providers based in the UK.</li> <li>Companies can be fined up to £18 million or 10 percent of their qualifying worldwide revenue, whichever is greater. Criminal action can be taken against senior managers who fail to ensure companies follow information requests from Ofcom.</li> </ul>	<ul style="list-style-type: none"> <li>Enacted on 26 October 2023.</li> <li>Started 25 July 2025 – Mandatory Age Verification for Adult Content</li> </ul>
IRELAND	<p>The Online Safety Framework is comprised of three different pieces of legislation:</p> <ul style="list-style-type: none"> <li>EU Digital Services Act</li> <li>Online Safety and Media Regulation Act</li> <li>EU Terrorist Content Online Regulation</li> </ul>	<p>Coimisiún na Meán is responsible for the online safety framework.</p> <p>Multi-person regulatory commission which oversees all content, including online safety, broadcasting &amp; video on-demand services.</p>	<p>Makes digital services accountable for how they protect people, especially children, from online harm.</p> <p>The framework aims to reduce the risk of people being exposed to illegal or harmful content online.</p>	<p>The Digital Services Act regulates service providers such as Apple, Google, Shein, LinkedIn, Meta, Microsoft, Pinterest, TikTok, Temu, X, Bing.</p> <p>Online Safety and Media Regulation Act regulates video-sharing platforms: Facebook, Instagram, YouTube, TikTok, and more.</p> <p>Terrorist Content Online Regulation regulates providers that store information e.g., social media platforms, cloud services, web hosting services.</p>	<p>The regulator can issue a penalty or fine of:</p> <ul style="list-style-type: none"> <li>6% of annual global turnover under the Digital Services Act.</li> <li>€20 million or 10% of turnover under the Online Safety Media Regulation Act, and</li> <li>4% of annual global turnover under the Terrorist Content Online Regulation.</li> </ul>	<ul style="list-style-type: none"> <li>Enacted on 10 December 2022</li> <li>Latest amendments are up to date as of 10 July 2025</li> </ul>

Figure 4: Approaches to addressing online harm in Australia, the United Kingdom, and Ireland.<sup>55</sup>

<sup>55</sup> This figure is included in advice provided by the Department of Internal Affairs.

## 4.2 Social media age restrictions

In December 2024, the Australian Government passed the Online Safety Amendment (Social Media Minimum Age) Act 2024.<sup>56</sup> The Act introduced age restrictions for social media platforms. From 10 December 2025, social media platforms will be required to take reasonable steps to ban users under 16 in Australia. This means that children under 16 will not be able to create or hold social media accounts in Australia. Courts can order civil penalties for online platforms that do not comply with these requirements.

The Government of Denmark has also declared its intention to ban access to social media for anyone under the age of 15.<sup>57</sup> Similarly, France introduced legislation in 2023 requiring platforms to verify users' ages and obtain parent consent before users under the age of 15 can use their platforms.<sup>58</sup>

As previously discussed, the Minister of Education is leading work to investigate restricting access to social media for users under the age of 16. Submitters offered a diverse range of views on this proposal. We heard both from young people who supported the idea and others who opposed it.

Some submitters also highlighted challenges involved in implementing this approach, such as the possibility that young people use a virtual private network (VPN) to bypass these restrictions.<sup>59</sup> Internet NZ cited research conducted by the Oxford Internet Institute that demonstrated that 68 percent of teenagers in the United Kingdom use VPNs to bypass age restrictions online. The Stratford District Youth Council said that restricting young people's access would "make social media even more unsafe". It expressed concern that if people under the age of 16 used social media and encountered harm, their ability to access support would be impeded.

The New Zealand Initiative also commented on privacy concerns related to young people being required to verify their age or identity online. It discussed the risks of online platforms or third parties gathering users' identification documents and personal information, in comparison to data being collected by a single authority that provides credentials or identification services. The New Zealand Initiative emphasised that age restrictions may just be evaded by young people and create burdens for those over the age limit to verify their age. Other submitters discussed how some level of privacy concern could be addressed if users were only required to verify their age to platforms, rather than providing further proof of identity or personal information.

## 4.3 Algorithm transparency

Similar jurisdictions to New Zealand have recently initiated attempts to address concerns regarding algorithm transparency. They include requiring online platforms to improve

---

<sup>56</sup> [Online Safety Amendment \(Social Media Minimum Age\) Bill 2024 | Parliament of Australia.](#)

<sup>57</sup> [Denmark plans social media ban for under-15s | The Guardian.](#)

<sup>58</sup> [France requires parental consent for under-15s on social media | Le Monde.](#)

<sup>59</sup> VPNs establish a digital connection between a person's computer and a remote server, creating a private connection for users that masks their internet protocol (IP) address and location.

accountability and access to information about how algorithms operate on their platforms. As these attempts are recent, it is difficult to assess how effective they have been.

Amendments to the Australian Privacy Act passed in 2023 introduced requirements for organisations, including online platforms, to disclose in their privacy policies when they use automated decision-making processes using personal data that could significantly affect the rights or interests of individuals.<sup>60</sup> The Australian eSafety Commissioner is also empowered to require online services to provide information about how their use of algorithms may contribute to or reduce the risk of online harm.

Legislation in the United Kingdom and Ireland relates to regulation of algorithms, but does not explicitly require transparency or public access to algorithms. While algorithms are not explicitly included in the United Kingdom's Online Safety Act 2023, platforms are required to design operations to protect users from illegal or harmful content. A code of practice established under the Act requires platforms to implement processes designed to prevent their algorithms from suggesting harmful content to children.<sup>61</sup> Similarly, the Online Safety and Media Regulation Act in Ireland regulates algorithms indirectly by requiring platforms to follow the Online Safety Code. An opposition political party in Ireland recently proposed an idea for a bill that would require social media platforms to turn off recommendation algorithms for users under the age of 18.<sup>62</sup>

The EU Digital Services Act includes requirements for social media platforms to grant researchers adequate access to public data stored on their platforms. On 24 October 2025, the European Commission "preliminarily" found both TikTok and Meta in breach of this obligation.<sup>63</sup> The Act also empowers the Digital Service Coordinators, who are responsible for enforcing the Act, to request information from very large online platforms and search engines to assess compliance. Digital Service Coordinators may require such platforms and search engines to "explain the design, the logic, the functioning and the testing of their algorithmic systems, including their recommender systems".<sup>64</sup>

## 4.4 Our response and reflections

In this section, we have provided a high-level overview of some international efforts to address online harm. We consider that New Zealand could benefit from assessing the lessons learned from other countries' approaches to regulating online activity, including any unintended consequences of these approaches. In particular, we consider it would be beneficial to further investigate and learn from international experiences with online age restrictions and algorithm transparency.

---

<sup>60</sup> [A spotlight on Australia Privacy Reform A long awaited first step First tranche privacy reforms | Bird & Bird.](#)

<sup>61</sup> [Quick guide to illegal content codes of practice | Ofcom.](#)

<sup>62</sup> [Bill to Turn Off Toxic Recommender Algorithms | People Before Profit.](#)

<sup>63</sup> [Commission preliminarily finds TikTok and Meta in breach of their transparency obligations | European Commission.](#)

<sup>64</sup> [Article 40, the Digital Services Act | European Commission.](#)

## 5 Our overall reflections and next steps

We acknowledge the time and effort of people who made a submission on this inquiry. We also thank the Department of Internal Affairs, which provided advice to us, and the Office of the Clerk, which provided procedural and administrative support.

In this interim report, we have discussed young New Zealanders' experiences of online harm and the current measures to address these risks. We intend to produce a final report in 2026 that concludes our overall findings and includes recommendations to the Government.

We summarise our overall reflections and intentions for further work below.

### **Understanding online harm**

We understand online harm as a complex and holistic issue, encompassing both the various types of harm encountered online, and the effects harmful content or activity may have on young people. Submitters spoke of a wide range of harms—from targeted alcohol advertising to sexual violence online. To address these issues, we consider it necessary to identify solutions that both target specific harms and address structural issues.

Submitters cited a wide range of evidence, including experimental studies, systematic reviews, surveys and interview studies, and lived experiences. We think it is important to consider what types of evidence should be used to inform policy responses. We consider that systematic reviews of research studies and meta-analyses should be weighted heavily when determining whether interventions are warranted. Equally, the effectiveness, workability, and proportionality of any solution should be analysed against the evidence. Overall, our view is that empirical evidence should be treated as the foundation for action and the primary source to inform policy development. We also recognise the value of considering people's lived experiences and advocacy expertise for ensuring that solutions are fit-for-purpose and appropriate to the communities they try to benefit.

We agree with submitters that high-quality research is needed that explores online harm in the specific context of New Zealand. Research may help us monitor trends and emerging challenges related to online harm and identify when interventions need to be made. We intend to explore in our final report ways that would encourage more New Zealand-based research.

### **Addressing the limitations of current legislation in New Zealand**

We intend to do further work to review current legislative settings and make recommendations for improvement in our final report. In particular, the majority of us consider that the approach to regulation in the Films, Videos, and Publications Classification Act and the Harmful Digital Communications Act is not fit for effectively regulating the online environment. The current approach enables individual pieces of content to be classified and addressed. The majority of us believe there could be benefit in taking a proactive, system-wide approach to social media platforms.

The majority of us consider that the safe harbour provisions, like those in the Harmful Digital Communications Act, combined with inadequate regulation means the online media companies effectively escape liability for the array of social harms caused by their businesses. We intend to further investigate ways in which a more robust set of legislated requirements on the online media companies, and a revised approach to the safe harbour provisions, could ensure that when the providers do not meet the requirements of the law they shoulder a more appropriate share of the liability through both the courts and statute.

We consider it necessary to explore banning or restricting “nudify” apps and/or further regulate the creation and distribution of pornographic images that display the likeness of children and young people. Although deepfake sexual images of children are covered under the Films, Videos, and Publications Classification Act as “objectionable” publications, we consider that there need to be stronger protections in this area. We consider it necessary to explore the option of banning or restricting “nudify” apps or further regulating the creation and distribution of sexual deepfakes in New Zealand. We will also examine what role a review of the Films, Videos, and Publications Classification Act and the Harmful Digital Communications Act could play in supporting this.

### **National regulator responsible for online safety**

We consider that we should explore introducing a national regulator that is centrally responsible for online safety. The majority of us contend there is a strong case that having a singular regulator will better enable young people and their parents and caregivers to seek support and know where to go for information on online harm. We intend to explore the potential effectiveness of this option and what it could look like, in our final report, alongside investigating other solutions. Preliminarily, we envision that the functions of a national regulator could include recommending additional obligations to be placed on online platforms and parents, and addressing non-compliance and complaints.

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.

### **Online platforms’ responsibilities**

We do not consider that online platforms are doing enough to address the gravity of the harm experienced. While submitters raised legitimate concerns about the effectiveness of platforms’ online safety tools, we also consider that platforms should do more to raise awareness of the features they already have available. We strongly encourage platforms to give users clear information about safety features and make them a more visible part of their platforms.

For these reasons, we intend to further consider whether the Government should play a stronger role in regulating the design of online platforms and mandating online safety features. We intend to examine the potential for regulatory tools to provide proportionate liability for online platforms. We plan to report our conclusions on this matter in our final report.

In particular, the majority of us consider there is a strong case that platforms should be made to provide more transparency on how their algorithms work. Algorithms operate in ways

typically obscured to users, making millions of decisions on their behalf. While there may be some benefits to personalising a user's experience, the majority of us believe the risk of algorithmic harm outweighs any advantage.

We also consider that stronger standards may be needed to prevent online advertising of harmful products reaching young people. We intend to further examine the relationship between online advertising of products like alcohol and young people's consumption of these products. We do not believe that online platforms should be able to display advertising content related to alcohol, tobacco, gambling, and other age-restricted products, to users under the age of 18.

### **Education and digital literacy**

We consider that there is a need to provide more educational resources to young people and their families. We are glad to see that there is more content related to digital technologies in the recent draft of the New Zealand Curriculum.<sup>65</sup> Responsibility for providing digital literacy resources to parents and young people is held by more than one group. For example, it may be that the Government, online platforms, independent researchers and universities, and educators should all play a role. We intend to further examine options for increasing digital literacy resources and training in New Zealand.

### **Learning from international experiences with age restrictions and algorithm transparency**

We are interested in seeing how implementation of the ban on under-16-year-olds using social media in Australia progresses. As these new restrictions come into effect from 10 December 2025, we hope to comment on some early reflections on the implementation process by early 2026. This is a topic we intend to give more attention to in our final report. However, preliminarily, the majority of us support restricting access to social media for under-16-year-olds. We accept the advice from some submitters that there are age verification challenges, and that some young online users will find ways around a ban. The majority of us nevertheless view that, while imperfect, the level of online harm currently being sustained by young people warrants introducing an age-delay restriction as part of a broader reform agenda.

The majority of us also support the idea of introducing requirements on online platforms to improve transparency and access to how algorithms operate, particularly for the purposes of public accountability. We understand that there are technical, legal, and privacy challenges in implementing approaches to improve algorithmic transparency, which we intend to examine further.

### **Our next steps**

We intend to focus our attention on further exploring the issues we have discussed above, as well as assessing other potential solutions that could address the concerns identified. In summary, the key reflections the majority of us agree require further consideration include:

---

<sup>65</sup> [Draft curriculum content released for Years 0 to 10 | Ministry of Education.](#)

1. restricting access to social media platforms for under 16-year-olds
2. regulating deepfake tools or “nudify” apps in New Zealand
3. whether New Zealand legislation, including the Films, Videos, and Publications Classification Act and Harmful Digital Communications Act, is fit for purpose
4. introducing a national regulator for online safety in New Zealand
5. ways in which regulatory approaches introduced in New Zealand could be made sufficiently agile to respond to new developments in technology as they occur
6. what role the New Zealand Government should play in regulating the design of online platforms
7. whether there is a need to restrict online advertising of harmful products, such as alcohol, tobacco, and gambling for under 18-year-olds
8. the level of liability online platforms and internet service providers should be held to for harmful and illegal content hosted through their services
9. the level of responsibility that parents should have in protecting their children from online harm, and the tools they would need to provide this support effectively
10. advantages and limitations of approaches to increase algorithm transparency
11. ways to learn from international experiences, including the implementation of the social media ban for under-16-year-olds in Australia
12. ways to encourage further research on online experiences in New Zealand.

The committee may also explore further ideas in addition to the ones described above.

### **Green Party of Aotearoa New Zealand differing view**

The Green Party of Aotearoa New Zealand support the majority of the potential solutions identified in the “our next steps” section above, but do not believe that restricting access to social media platforms for under-16-year-olds would address the concerns identified.

### **ACT New Zealand differing view**

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

In May 2025, Dr Parmjeet Parmar MP wrote to the committee asking that such an inquiry be initiated, reflecting widespread concern about the challenges raised by parents, experts, and members of the public.

This interim report was intended to summarise the information and advice “received relating to young people’s experiences of online harm, and provide an overview of current efforts to address online harm in New Zealand”. It provides for an assessment of the harms and benefits of social media as raised by submitters, an evaluation of the regulatory environment, and a mapping of the current landscape.

However, ACT is concerned that the interim report has drifted noticeably from its intended purpose. Rather than simply laying the groundwork of understanding the issue at hand for a more comprehensive second report in early 2026, the interim report leans heavily into recommendations on policy options. This is premature and risks compromising the quality and integrity of the final report.



Additionally, the committee has not yet adequately engaged with several important elements of the inquiry's terms of reference. In particular, the interim report does not meaningfully evaluate the effectiveness of current measures in reducing the incidence or severity of online harm among young people. Nor does it adequately examine whether the limitations of existing harm-reduction efforts result from flawed design, insufficient resourcing, or simply a lack of uptake and engagement. These questions are foundational and set out in the terms of reference. Without understanding what currently works or fails and why, no responsible policymaker can justify proposing new layers of regulation.

This analytical gap is made more concerning by the report's premature signalling of strong support for significant new interventions, such as the establishment of a national regulator or an age-based social media ban.

The committee has not yet provided a clear or coherent definition of "social media". The report acknowledges conceptual difficulties but nevertheless makes recommendations that require a stable and consistent definition. As it stands, the current attempt at a definition would include virtually the entire internet.

The international policy environment is changing rapidly. Countries such as Australia are preparing to introduce major interventions, including a proposed ban on social media for those under 16. New Zealand should observe these developments before committing to similar measures. A pragmatic approach would allow policymakers to learn from overseas successes or failures rather than repeating mistakes that become apparent only after implementation.

The initial impacts of Australia's legislation will be evident prior to the committee's discussion on possible solutions.

ACT recognises that young people face real and significant harms online. The primary responsibility for preventing those harms rests with parents and caregivers, whose decisions about children's access to devices are the most direct and effective safeguard. Limiting device use is often more impactful than regulating specific apps or platforms.

That said, ACT accepts that there may be a legitimate role for other parts of society, including Government, provided that any intervention meets high standards of proportionality, effectiveness, and respect for individual rights and freedoms.

Any recommendations should be reserved for the final report, where evidence has been fully digested and thoughtfully considered, and the committee should not seek to limit the options available to it when considering possible solutions.

Nothing in the interim report should be relied upon to determine policy before the committee releases its final report in early 2026. A high-quality final report must rest on clear definitions, a proper evaluation of existing measures, a comprehensive analysis of evidence, and a disciplined separation between inquiry and advocacy.

For these reasons, while ACT agrees with the report about the harms young people face online and remains open to workable solutions, ACT cannot support the premature conclusions contained in the interim report and urges the committee to return to the analytical foundations required for a credible and robust final report.

## Appendix A: Committee procedure

### Committee procedure

We initiated this inquiry on 4 June 2025 and are continuing to consider it. We called for public submissions between 26 June and 30 July 2025. We received submissions from 400 organisations and individuals and heard oral evidence from 87 submitters. We have received advice from the Department of Internal Affairs.

### Committee members

Katie Nimon (Chairperson)

Carl Bates (Deputy Chairperson)

Shanan Halbert

Francisco Hernandez

Grant McCallum

Dr Parmjeet Parmar

Hon Willow-Jean Prime

Hon Phil Twyford

Dr Vanessa Weenink (Acting Chairperson from 16 July to 8 August 2025)

Mike Butterick, Reuben Davidson, Hūhana Lyndon, and Dr Lawrence Xu-Nan 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 \(2024\).](#)