



The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand

What is it, how are children and youth engaging with it, and how do we keep them safe?

Contents

Executive summary	3	1. HOW YOUNG PEOPLE ENGAGE ONLINE	15	3.6 Self-generated sexual content and AI companions	45
Key findings	4	1.1 International data	16	3.7 Influence of TV and mainstream media	46
Recommendations	8	1.2 Aotearoa New Zealand data	17	4. THE AOTEAROA NEW ZEALAND CONTEXT	48
Authors' note	13	1.3 Youth feedback and insights in Aotearoa New Zealand	18	4.1 Existing agencies	49
Introduction	14	2. THE NEW YOUTH DIGITAL SEXUAL LANDSCAPE	20	4.2 Youth and FVSV sector feedback: Trends and harms	53
		2.1 'Mainstream' porn sites	21	4.3 Youth and FVSV feedback: Skills and capabilities	55
		2.2 Child sexual abuse material (CSAM) and objectionable content	24	5. AOTEAROA NEW ZEALAND REGULATORY AND POLICY APPROACHES	56
		2.3 Bestiality and rape-related content	26	5.1 Aotearoa New Zealand	57
		2.4 Online reading, writing, and story-sharing communities	26	5.2 International regulatory overview	59
		2.5 Generative AI and AI-generated platforms	27	6. TECHNOLOGY AND INDUSTRY	68
		2.6 Extended reality platforms	28	6.1 Technology initiatives that address sexual abuse and interactions	69
		2.7 Social media and messaging apps/platforms	30	6.2 Overview of built-in parental controls	70
		2.8 Mainstream streaming services	31	6.3 Safety by design	72
		2.9 Dating apps	33	6.4 Further investment needed in research & development	74
		2.10 Platforms for self-generated sexual content	34	7. RECOMMENDATIONS	75
		2.11 Children's sites and gaming	34	7.1 System, leadership, and learning	76
		3. WHAT ARE THE RISKS AND HARMS?	36	7.2 Capability and coordination	82
		3.1 Technology-facilitated sexual violence	37	7.3 Action in the community	85
		3.2 Exposure to CSAM and changing sexual norms	40	REFERENCES	88
		3.3 Shifts in sexual attitudes, beliefs and behaviours	42		
		3.4 Increased risk of female victimisation	44		
		3.5 Accelerated risk of harmful sexual behaviour (HSB) in vulnerable youth	44		

Executive summary

The digital world has transformed how young people in Aotearoa New Zealand access information, build relationships, and express themselves. From mainstream streaming services to virtual reality, the internet offers unparalleled opportunities for education, connection, and creativity. However, alongside these opportunities, the digital environment presents profound risk, particularly in the realm of sexual exploitation, abuse, and the development of harmful sexual norms around violence.

Young people's engagement with digital platforms is driven by curiosity, social pressures, and a natural desire for connection and validation. However, the accessibility, anonymity, and unregulated nature of online spaces can heighten their vulnerability - exposing them to explicit sexual content, pressure to create sexual material, image-based abuse, and harmful sexual norms, with significant risks to their wellbeing, development, privacy, and safety.

The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand examines how youth engage with this complex environment, with a specific focus on the harms arising from exposure to explicit sexual content, unsafe design features, and contact with predatory bad actors.

Overall, it demonstrates that in the digital age, sexual harm is no longer confined to offline spaces. The digital environment now exposes children and young people to new and diverse forms of sexual harm. These include harms occurring online such as technology-facilitated sexual violence (TFSV), image-based abuse (IBA), and exposure to harmful sexual content and CSAM.

There are also intersecting harms, where digital experiences are entwined with offline abuse, for example, when self-generated content is weaponised through sextortion, or when grooming occurs in unmoderated online spaces. Most critically, systemic harms are emerging, as ongoing exposure to pornography, CSAM, and harmful sexual norms can shape some young people's attitudes and behaviours - contributing to a rise in offline harms such as rough sex and 'choking' / sexual strangulation.

Key Findings

The online-related risks faced by young people centre around, but are not limited to, four key areas:

These risks undermine young people’s safety, wellbeing, and digital rights, and collectively contribute to a rise in the types of sexual harms linked to digital technologies.

ONLINE RELATED RISKS FACED BY YOUNG PEOPLE

Content:

Exposure to harmful material and its influence on norms, attitudes, and behaviours

Contact:

Such as online grooming or sextortion

Conduct:

Including abusive messaging or sexual harassment

Contract:

Agreeing to exploitative or harmful terms on digital platforms

Content

In the United Kingdom, the majority of young people reported to have seen porn by 13 years of age and in the United States, the average age of exposure to porn is 12

[BBFC, 2020; Common Sense Media, 2023].

Older research conducted in New Zealand found that 25% of youth first saw porn at age 12 or under, and 71% who had encountered pornography did so unintentionally

(Classification Office, 2018).

ANALYSIS OF MAINSTREAM PORNOGRAPHY CONTENT HAS SHOWN:

- Sexual aggression is widespread in mainstream porn. 45% of scenes contain physical or verbal aggression (Fritz, 2020).
- Sexual violence, coercion, deception, and criminal activity are positioned as mainstream and permissible (BJC, 2020).
- In Aotearoa, 35% of the top-viewed Pornhub videos involved coercive or non-consensual behaviour and 46% included incestual/family themes (Classification Office, 2022).

Critically, exposure to this content can shape young people's attitudes, expectations, and behaviours around violence - contributing to a rise in online and offline sexual harms.

THE IMPACTS OF PORN AND VIOLENT CONTENT ON BELIEFS AND BEHAVIOURS AROUND VIOLENCE:

- Regular porn users are more likely to develop attitudes that support violence, adopt rigid gender roles, sexist attitudes and scripts in porn, and accept sexual aggression and rape myths (Upton, 2020).
- Regular viewers are 4 - 10 times more likely to perpetrate four types of aggression: sexual harassment, sexual coercion, forced sex, and/or manipulative sex, and display decreased bystander willingness (Upton, 2020).
- The normalisation of online sexual violence can reinforce and accelerate harmful sexual behaviours, and shape young people's perceptions, expectations and experiences of violence (Mori, 2023).

Exposure to CSAM is linked to increased risks of child contact, desensitisation, and normalisation of sexual aggression, with some genres of mainstream pornography contributing to the sexualisation of children and misconceptions about consent.

FINDINGS INCLUDE THE FOLLOWING:

- **CSAM and contact risks:** 42% of individuals consuming CSAM reported seeking direct contact with children via online platforms after viewing CSAM.
- **Violent content concerns:** Regular consumption raises concerns about desensitisation and the normalisation of sexual aggression and predation.
- **Desensitisation and mainstream pornography:** 12% of CSAM offenders cited desensitisation from viewing mainstream pornography as a factor in their pursuit of CSAM. (Insoll et al., 2024)

Contact:

- **Online grooming:** At least 1 in 10 young people experience online grooming (Schittenhelm et al., 2024).
- **Self-generated CSAM:** 13% of minors reported they had a friend who had received money or gifts in exchange for self-generated CSAM, while another 7% selected “prefer not to say” (Thorn, 2023).
- **Online sexual interaction:** 1 in 3 young people reported having an online sexual interaction; 1 in 5 believed it to be with an adult (Thorn, 2023).

Conduct:

- **Image-based abuse:** 1 in 3 people reported that someone had taken a nude or sexual image of them without their consent (Henry et al., 2021).
- **Sextortion:** 1 in 10 Australian adolescents said that someone had sexually extorted them for money or more intimate material (Wolbers et al., 2025).
- **'Nudify' apps** are becoming increasingly popular and used to create non-consensual deepfakes, and AI chatbots can perpetrate sexual abuse without identifiably human motives. Tech platforms target not only youth attention but also their intimacy.

Contract:

Almost all platforms and websites researched ask for consent to terms and conditions before they can be accessed, but it is a risk factor for children to accept terms and conditions they don't understand.

It is also important to note that beyond these four key areas of risk, emerging technologies and platforms are giving rise to new and evolving areas of risk. While evidence is still emerging, early research suggests that engagement with online subcultures such as the BookTok Dark Romance community may increase vulnerability to female victimisation. AI-generated social companions also show potential to reinforce harmful sexual behaviours and relational dynamics. Additionally, systemic harms are increasingly linked to the way pornography reflects and reinforces the drivers of sexual violence.

Workforce feedback from Aotearoa New Zealand indicates a clear rise in harms across these risk areas, alongside a lack of adequate support and protection for young people.

Key findings include:

- **A marked increase in TFSV**, shifting sexual norms around violence, and online-related harms such as rough sex and 'choking' / sexual strangulation.
- **Major gaps in Family Violence Sexual Violence (FVSV)** workforce knowledge and skills regarding online sexual harm and pornography. Only 14% rate their knowledge as 'good,' while 83% report their service lacks adequate capability (FVSV Scoping Report, 2024).
- **A lack of support and guidance for young people navigating the digital landscape.** Two-thirds report never having spoken to a parent or caregiver about porn - often due to fear of stigma, shame, or punishment (Classification Office, 2018).

The digital sexual landscape and subsequent emerging harms are now a critical dimension of FVSV amongst children and young people in Aotearoa New Zealand - by providing conditions that can create, contribute to, and perpetuate harm. Urgent recognition of this shift is required by government agencies, the sexual violence sector, and communities. It also has significant implications for the FVSV sector's obligations under Te Aorerekura to address the conditions that create harm, and to ensure young people are protected and supported to live lives free from violence.

Recommendations

As young people engage across an increasingly diverse range of platforms, our societal response must evolve to reflect this complexity. Our children and young people are exposed to ever-increasing risk of sexual harm online. At present, Aotearoa is failing to meet its obligations under the United Nations Convention on the Rights of the Child to uphold children's rights in the digital environment. These recommendations seek to rectify this so that children and young people can navigate the internet safely in the future.

“The rights of every child must be respected, protected and fulfilled in the digital environment.”

(United Nations Committee on the Rights of the Child, General comment No 25, 2021)

1. Broad consultation with diverse stakeholder groups
2. Legislation and policy reform
3. Research, monitoring, and evaluation
4. Workforce and organisational development
5. National digital sexual landscape resources
6. Action in the community
7. Education for young people
8. Social norms around internet and device use
9. Investment in innovation is needed to reduce online-related harm
10. Tailored support for priority groups

1. Broad consultation with diverse stakeholder groups

A process of reform should be undertaken to address the issues of online safety for children and young people in Aotearoa New Zealand. The process of reform should begin with broad consultation with key stakeholder groups, honouring Te Tiriti o Waitangi obligations and ensuring adequate Māori representation in all levels of leadership and delivery.

This work was started by the Safer Online Services and Media Platforms (SOSMP) review, which provides a solid foundation for this consultation process.

Broad stakeholder engagement is necessary and should include:

- **tech platforms** (e.g., Meta, Google, TikTok, Discord)
- **Internet Service Providers** (ISPs)
- **non-governmental organisations and advocacy groups** (e.g., Safeguarding Children, Netsafe, Rape Prevention Education)

- **youth** (e.g., Whāraurau youth advisors, Rainbow Youth, VOYCE)
- **education providers**
- **community representatives and free speech advocates**
- **health professionals, specialist organisations, and researchers** in child wellbeing, trauma, and digital safety.

Stakeholder engagement should be nationally representative, including feedback from minority groups such as LGBTQIA+, religious groups and ethnic groups.

2. Legislation and policy reform

New Zealand urgently needs a national response to online sexual harm, one that brings together legislation, education, and industry responsibility.

A stronger, coordinated framework must replace the current voluntary approach, which is failing to protect our children.

From the foregoing analysis of the digital sexual landscape and young people in Aotearoa, we recommend four key pillars for reform:

- Develop and publish a **National Strategy to Address Online Child Sexual Abuse and Online Related Harm**. This would require a multi-agency, whole-of-society approach to ensure its effectiveness.
- Develop a comprehensive **Children's Online Safety Act** to establish a clear legal framework for online child protection.
- Establish a **Children's Online Commissioner** to lead and oversee enforcement and advocacy and maintain a strong regulatory framework to protect children and young people from harmful online experiences.

- Establish a **Centre for Children's Online Safety** as a dedicated national agency for children's online safety leading strategy, education and coordination. The Centre would bring together all key stakeholders, including agencies, educators, tech firms, child protection experts, and families. It would also promote digital literacy and safety education in schools and homes, empowering parents and teachers to guide children's online activity. The Centre would encourage international collaboration through multi-lateral forums such as OECD and UN bodies to align global standards and share best practices.

3. Research, monitoring, and evaluation

International best practice shows that robust data is key to a national approach to tackling child sexual abuse.

Over 80% of countries surveyed by UNICEF (2022) collect data on child sexual exploitation, including technology-facilitated abuse, which helps set baselines and guide national responses. Research can inform interventions and policies, but all research must remain free from industry influence to maintain trust and integrity.

4. Workforce and organisational development

Nationwide workforce and organisational development is recommended to build confident, skilled and well-equipped FVSV, health, youth, justice, education, and social services.

Workforce development should include evidence-based, foundational and specialised training, alongside training resources to guide and inform workplace prevention, assessment and response initiatives relating to the digital sexual landscape.

5. National digital sexual landscape resources

The development of a central suite of national resources for FVSV, health, youth, justice, education, and social services is recommended.

These should encompass evidence-based information, tools and response pathways to support sector practice, prevention and response initiatives related to the digital sexual landscape.

6. Action in the community

Nationwide campaigns must actively engage parents across all school-age groups, working in partnership with existing community groups to ensure messages are relevant, trusted, and grounded in local realities.

These campaigns should offer clear, age-appropriate guidance on introducing devices, while equipping parents with practical tools to navigate the risks of early digital exposure, promote safer alternatives, and foster online protective factors. As digital trends rapidly evolve e.g. the rise of AI companions, parents face growing blind spots that leave children and young people vulnerable. Ongoing, community-led investment in digital literacy is essential to effective, long-term harm prevention.

7. Education for young people

While caregivers and policy play key roles, schools are essential in teaching children aged 7+ to navigate online risks and foster positive understanding of sex and gender.

Early, repeated, and interactive education on consent, privacy, and empathy builds resilience and helps children recognise and resist coercive behaviours - whether from predators or through normalised messages in harmful online sexual content. For teens, a strengths-based, ethical sexual citizenship approach fosters critical thinking and protects against harmful online sexual content.

8. Social norms around internet and device use

Current social norms around internet and independent device use, such as early device ownership, unrestricted app access, and bedroom use are not cautious enough given the risks of online sexual harm.

Keeping school devices on-site until high school can shift these norms by reinforcing that digital access is for learning, while also limiting unsupervised home use and reducing reliance on parental controls, especially since school filters don't apply off-site. Reducing harm is also linked to socioeconomic factors, with structured after-school activities helping to build resilience and protective networks while offering safer alternatives to screen time.

9. Investment in innovation is needed to reduce online-related harm

Investment in research and technological advancements will be essential to stay ahead of emerging AI threats.

Innovative solutions are needed to combat sextortion, online grooming, CSAM, AI-generated CSAM, wider objectionable content and other online-related harms. Real-time insights can inform timely interventions and policies. A dashboard could present emerging risks to inform parents, educators, and industry.

10. Tailored support for priority groups

When designing online safety campaigns and interventions, it is essential to consider the specific needs and experiences of priority groups who may face heightened risks or barriers to support e.g. low-income families, children with disabilities or neurodivergence, and children in rural communities.



Author's Note

This report highlights the critical need to protect young people from digital sexual harms while at the same time empowering them to navigate the internet safely. It calls for robust policies, education and collaboration between government, tech industries and communities to mitigate risks.

By addressing these challenges, the sexual violence sector can safeguard Aotearoa's youth, ensuring the digital world is a space of opportunity rather than exploitation.

The report is a collaboration between Safe Surfer and Makes Sense, with The Light Project providing content contributions to Sections 1 - 4. It is important to note that the authors were not commissioned to undertake any consultation with stakeholders. This may mean there are initiatives we are unaware of, or research we have not been privy to. However, for many years Makes Sense and Safe Surfer have engaged with stakeholders in their capacity as advocates to hear many perspectives around online harm in relation to sexual content, and some of these perspectives and themes have informed our high-level recommendations, alongside academic research and evaluations of successful international programmes.

Consultation is vital as a next step to address this evolving landscape, recognising the diversity of stakeholder perspectives.

While broad engagement will shape effective and balanced strategies, achieving full agreement on strategy and intervention is not guaranteed.

The authors also recognise the potential cultural biases within our Pākehā-led organisations. Our recommendations therefore emphasise a robust Te Tiriti o Waitangi approach, prioritising meaningful engagement with iwi, hapū, whānau, and rangatahi to collaboratively shape future actions.

Introduction

The digital world has transformed how young people in Aotearoa New Zealand access information, build relationships, and express themselves.

From mainstream streaming services to virtual reality, the internet offers unparalleled opportunities for education, connection, and creativity. However, alongside these opportunities, the digital environment presents profound risk, particularly in the realm of sexual exploitation, abuse, and the development of harmful sexual norms around violence.

Young people's engagement with digital platforms is driven by curiosity, social pressures, and a natural desire for connection and validation. However, the accessibility, anonymity, and unregulated nature of online spaces can heighten their vulnerability - exposing them to explicit sexual content, pressure to create sexual material, image-based abuse, and harmful sexual norms, with significant risks to their wellbeing, development, privacy, and safety.

The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand examines how youth engage with this complex environment, with a specific focus on the harms arising from exposure to explicit sexual content, unsafe design features, and contact with predatory bad actors.

Overall, it demonstrates that in the digital age, sexual harm is no longer confined to offline spaces. The digital environment now exposes children and young people to new and diverse forms of sexual harm.

These include harms occurring online such as technology-facilitated sexual violence, image-based abuse, and exposure to harmful sexual content and CSAM.

There are also intersecting harms, where digital experiences are entwined with offline abuse, for example, when self-generated content is weaponised through sextortion, or when grooming occurs in unmoderated online spaces. Most critically, systemic harms are emerging, as ongoing exposure to pornography, CSAM, and harmful sexual norms can shape some young people's attitudes and behaviours – contributing to a rise in offline harms such as rough sex and 'choking' / sexual strangulation.



1

How young people engage online

This section presents a broad summary of youth behaviour around online sexual content, highlighting trends, drivers and, where possible, feedback and data specific to Aotearoa New Zealand.

It outlines how youth engage with sexual content and what motivates or influences their behaviour online. We point out here that the existing research and data typically focus on adolescents because ethical considerations prevent introducing adult concepts to younger children to avoid potential harm.

1.1 INTERNATIONAL DATA

Globally, there has been a seismic shift in how young people engage with the digital world.

In 2024, online engagement deepened, driven by increasing access to smartphones, gamified platforms, and hybrid learning environments.

Teenagers are among the most active users of the internet globally. In the United States, 97% of teens use it daily and 46% use it “almost constantly” (Faverio & Sidoti, 2024). In addition, 95% of teens have or have access to a smartphone, 90% a desktop or laptop computer, and 83% a gaming console (usually internet-search-enabled) (Anderson et al., 2023).

Key trends include rising participation in online gaming, higher rates of social media use, growing exposure to cyberbullying, and concerns around digital wellbeing. Education systems and guardians face a growing need to balance the benefits of digital interaction with emerging risks.

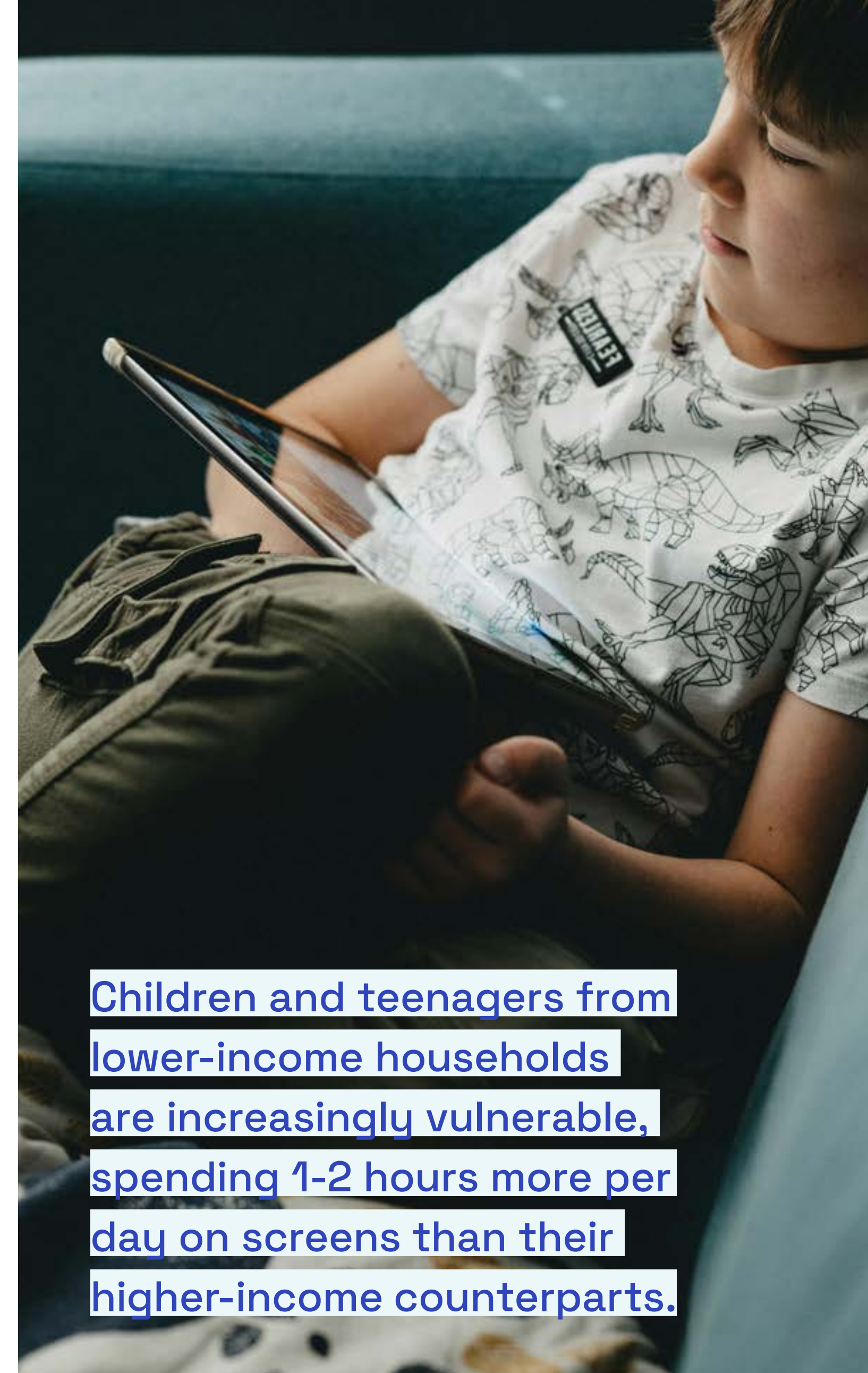
Children and teenagers from lower-income households are increasingly vulnerable, spending 1-2 hours more per day on screens than their higher-income counterparts. Despite higher-income households having greater access to devices, lower-income youth use them more extensively. This suggests that the affordability of alternative activities (e.g., sports, extracurriculars) and differences in parental oversight may drive the disparity (Common Sense Media, 2019, Ofcom, 2020).

There has also been a significant rise in online engagement among younger children, with those aged 5-8 now averaging 3.28 hours of screen time per day (Common Sense Media, 2021). 75-80% of caregivers are worried about screen time use and content exposure, however device and platforms access has only continued to rise (Common Sense Media, 2021; Funk et al., 2020; Parents Together Action, 2021).

“Digital inclusion must come with digital protection. No child should ever pay the price of progress with their safety.”

(Dr Doreen Bogdan-Martin, Secretary-General of the International Telecommunication Union, World Summit on the Information Society, 2024)

Children and teenagers from lower-income households are increasingly vulnerable, spending 1-2 hours more per day on screens than their higher-income counterparts.



1.2 AOTEAROA NEW ZEALAND DATA

The use of digital technologies, including handheld devices and computers, is increasing rapidly among New Zealand children.

Between 2012 and 2018, the global rate of digital use among children increased from 21 to 35 hours per week; in New Zealand, it increased from 22 to 42 hours (Cullen et al., 2024; OECD, 2021).

Recent research produced for the Ministry of Social Development found higher levels of screen time among Māori, Pasifika and Asian children in New Zealand (Gath et al., 2023). This is consistent with the trends identified in the international research cited above: the factors contributing to this include the prohibitive cost of alternative activities (e.g., sports, extracurriculars) and different parenting styles, as well as socioeconomic deprivation.

“Young New Zealanders are reported to be among the highest digital users in the world both at home and in school.”

(OECD, 2021; Cullen et al., 2024)

In June 2022, the Classification Office published a report entitled **What We’re Watching Now** based on research among 1,001 adults and 200 teenagers seeking their views about what New Zealanders see on-screen and online. Key findings included:

Most New Zealanders are concerned about children and young people seeing harmful or inappropriate content in movies, shows and video games (74%), while 83% are concerned about content in other online spaces, such as social media.

Depictions of sexual violence or sexual harassment (95%) and self-harm or suicide (94%) were seen as especially harmful, along with racist comments, behaviour or stereotypes (91%), and realistic violence (91%).

97% believed that content in movies, shows and games can have a negative influence on children and young people’s attitudes or emotional wellbeing in various ways.

While there was widespread support for regulating harmful content, just 43% ‘somewhat’ or ‘strongly’ agreed that the current system of media regulation in New Zealand is working well to keep young people safe from inappropriate or harmful content online.

Participants were also questioned on the need for better regulation and government action, with findings showing that the most pressing issue was social media as well as other online content. Some wanted stricter measures to hold tech companies to account while others talked about legal requirements for online age restrictions.

1.3 YOUTH FEEDBACK AND INSIGHTS IN AOTEAROA

Research into young people’s experiences with porn and digital sexual engagement in Aotearoa remains limited due to ethical constraints, social taboos, and gaps in adult understanding of the rapidly evolving digital landscape. Youth perspectives provide critical insights, not only in identifying current risks and harms but also in informing effective solutions.

The following summary of New Zealand youth feedback has been drawn from a range of sources, including the Classification Office’s Youth and Pornography research series (Classification Office 2018, 2020) University of Auckland research (Meehan, 2024) Youth Digital Wellbeing survey (Digital Waitaha, 2024) and The Light Project’s youth surveys and focus groups (The Light Project 2018, 2022).

1.3.1 Young people want to be heard

Young people report that porn, sexualised media, and online sexual engagement are now an unavoidable part of youth sexual culture. They go online to learn, explore and connect sexually with the digital world increasingly integrated into their sexual experiences and relationships. Many recognise the challenges and risks and pressures, think critically about them, and want to be heard and included in shaping any solutions to address them.

1.3.2 Porn and sexualised media as ‘Sex Ed’

Many young people describe using porn and sexualised media as a main source of sex education, with 1 in 5 having tried something they’ve seen in porn and 73% of regular viewers using it as a learning tool. Others describe engaging with porn for entertainment, arousal, because of peer pressure, or to manage negative emotions like stress or anxiety.

1.3.3 Harmful and unwanted exposure

Most young people are first exposed to porn at or by age 12, often accidentally through pop-up ads or social media. Over 70% report seeing violent or non-consensual content and highlight the pervasiveness of racism, sexism and queerphobic content. In addition, 78% describe feeling uncomfortable around what they see, with many lacking trusted adults to help them process their experiences.

1.3.4 Impacts on sexual norms and mental health

Most young people acknowledge porn’s influence and say it distorts ideas of sex, gender roles and relationships. Some believe it is normalising risky and violent sexual behaviours, particularly towards girls, and creating new trends such as rough sex and ‘choking’ / strangulation. Others report impacts on their mental health such as anxiety, shame or feeling “addicted” to porn. Among regular porn viewers, 43% want to reduce their usage but struggle to do so.

1.3.5 Unwanted online sexual experiences

Unwanted online sexual experiences are common. These include pressure to send nudes, non-consensual image sharing, unsolicited sexual images, bribery, harassment, and unwanted sexual contact. Young people often turn to friends for support rather than adults, citing shame and fear of judgement as key barriers.

1.3.6 Normalisation of nudes and selling sexual images

Young people describe sharing nudes as a normal part of flirting and relationships, while also noting that non-consensual sharing is common and can lead to shame, anxiety and social fallout. Many also observe the growing appeal and romanticisation of selling sexual images on platforms like OnlyFans, despite risks such as bullying, harassment, stalking and regret.

1.3.7 AI sexual apps and deepfakes

Young people report growing engagement with a range of AI-driven sexual platforms, particularly AI boyfriend/girlfriend apps due to their personalised, constant companionship and validation. However, they also report concerns around secretive, addictive and sexualised relationships with AI companions, and the rising creation and sharing of non-consensual AI deepfakes.

1.3.8 Unique needs of Rainbow youth

Rainbow youth report unique and often conflicting experiences with online sexual content. Many use it to explore and affirm their identity due to gaps in inclusive sexuality education and are more likely to turn to porn as a learning tool. However, the prevalence of fetishised, violent or non-consensual content in queer porn can be confusing and distressing – and many lack support to process it.

1.3.9 Lack of adult guidance and support

Young people want and need evidence-based support and guidance on the digital sexual landscape. However, two-thirds report never having spoken to a parent or caregiver about porn, often due to fear of shame, stigma or punishment.

The lack of adult guidance alongside common abstinence-focused approaches can make it difficult for young people to manage risks or seek help when harm occurs. As a result, many report turning to peers or going online for information, often feeling unprepared and unsupported in navigating their online sexual experiences.



2

The New Youth Digital Sexual Landscape

This section provides an overview of the platforms where young people encounter or interact with sexual content. It also explores platform types, content, trends, accessibility, and usage patterns.

“The growth of the internet and social media has led to an explosion of content, much of which is user-generated. Engagement-maximising algorithms amplify harmful content, and bad actors can exploit these advancements to increase the reach and spread of harmful material, leading to real-world harm.”

(Classification Office, 2023)

2.1 'MAINSTREAM' PORN SITES

Mainstream pornography platforms emerged in the mid-2000s, paralleling the rise of video-sharing platforms like YouTube.

The infrastructure of these platforms allows for the hosting and serving of limitless content, often free of charge. The three most popular porn sites in Aotearoa are Pornhub.com, XNXX.com and XVideos.com. These websites command 60% of the total web traffic for mainstream porn sites globally. The remaining 40% of web traffic to adult websites is estimated to be across 5 million commercial adult porn sites (BBFC, 2018).

The scale and success of the dominant players is based in a complex web of interconnected websites scaled across hundreds of millions of backlinks and referral sites to facilitate affiliate marketing campaigns and financial transactions.

Porn is legal in New Zealand but restricted to those over the age of 18. However, all mainstream porn sites are easily accessible without having to verify users' age.

Young people report being just as likely to be exposed to porn on a variety of social platforms, such as X (formerly Twitter), YouTube and Reddit, as on dedicated pornography sites.

A growing body of evidence highlights the alarming rates of pornography exposure among young people. In the United Kingdom, the majority of young people reported having seen porn by 13 years of age, and in the United States the average age of exposure to porn is 12 years old (BBFC, 2020; Common Sense Media, 2023).

Older research conducted in New Zealand found that 25% of youth first saw porn at age 12 or under, and 71% who encountered pornography did so unintentionally. Furthermore, a significant percentage of young viewers have been exposed to violent or non-consensual sexual content (Classifications Office, 2018).

Young people in the United Kingdom aged 16-21 years said that they encountered violent and pornographic content online without seeking it out. Focus group studies revealed it made young people “confused”, “insecure”, “troubled”, “shocked”, “upset” and “curious”.

Additionally, some spoke about the role of sexualised cartoons, often featuring popular cartoon characters, which appear in pop-up ads. The report concluded that curious young people are being pulled into early sexual discovery by the profit-driven porn industry (Children's Commissioner's Office for England, 2023).

2.1.1 What’s in free mainstream porn?

Free online pornographic sites have significantly altered the nature of pornography in recent decades.

Pre-internet, pornography was restricted, limited in distribution, and depicted more conventional sexual behaviours. In contrast, today’s digital platforms provide children and young people with unrestricted access to a vast and largely unregulated array of content, where themes such as sexual violence, misogyny, coercion, and familial sex are pervasive.

This shift towards more sexually violent content has been driven by market saturation, competition, algorithms, lack of regulation, and social trends. With billions of free porn videos online, producers increasingly rely on extreme and novel content to attract viewers, boost advertising, and generate revenue.

While sexual violence is pervasive on mainstream porn sites, there is a growing genre of ‘better’ or ‘alternate’ porn which generally offers more ethical content. However, young people in Aotearoa rarely access these sites due to cost and platforms imposed age restrictions.

AVERAGE MONTHLY WEB VISITS BY NEW ZEALANDERS FOR THE COUNTRY’S THREE MOST POPULAR MAINSTREAM PORN SITES (2022–2023)

	MONTHLY UNIQUE VISITS	AV. TIME PER VISIT	AV. NO.OF PAGES VISITED
	1.08 MILLION	 9 MIN 34 S	 8.3
	871,000	 14 MIN 52 S	 11.6
	975,000	 11 MIN 55 S	 8.0

Source: Semrush data, 2022–2023.

Note: Monthly unique visits represent unique internet protocol (IP) addresses, not a representation of access per population. More than 95% of visitors were from mobile devices.

The following are key themes prevalent across free mainstream porn sites.

While many young people may not actively seek out this content, it's difficult for them to avoid.

- **Sexual aggression and coercion:** Sexual aggression is widespread in mainstream porn. A recent study of 130,000 titles across popular free sites concluded sexual violence, coercion and criminal activity are now positioned as mainstream and permissible (BJC, 2020). Other studies have found 45% of scenes contain physical or verbal aggression (Fritz et al., 2020), and, in Aotearoa, 35% of the top-viewed Pornhub videos involved coercive or non-consensual behaviour (Classification Office, 2019).
- **Aggression depicted as pleasurable:** Physical and verbal aggression are almost always (97%) directed towards women and female actors are generally depicted as enjoying being subject to violence (Bridges, 2010). Women, performers labelled "teen", and sexuality and gender-diverse performers are more frequently the targets of physical aggression.
- **Non-consent:** Explicit consent is rarely seen in porn. Non-consensual sexual behaviour is a central theme in mainstream porn and common scripts including being manipulated, tricked, or dominated into sexual activity.
- **Family-themed sex scenes:** Incest and family sex is a popular genre of porn. In Aotearoa, 46% of the top viewed Pornhub videos in 2020 involved family or stepfamily sexual activity or fantasy (Classification Office, 2019).
- **Diverse sexual behaviours (e.g., 'choking' / strangulation):** Diverse sexual behaviours such as rough sex, 'choking', group sex, and unconsented anal sex are commonly depicted in mainstream porn. They are generally portrayed as normative, pleasurable, and any potential risks are minimised.
- **Racist portrayals of people of colour:** Many porn sites contain racist stereotypes and depictions. Recent content analyses indicate Black and Asian men are five times more likely to be shown as aggressors, and Asian and Latina women are more often targets of aggression (Fritz, 2021; Seida, 2021).
- **Portrayals of sexuality and gender diversity:** Mainstream queer porn, often produced for heterosexual male audiences, is commonly characterised by high levels of aggression and non-consensual acts, along with transphobic, biphobic, and homophobic stereotypes. Sexuality and gender-diverse actors are more frequently targets of aggression and more likely to be fetishised (Seida, 2021).

- **Teen sex:** Young, childlike and teen (18-year-old) sexual themes are common in porn, with a 2020 study indicating 'teen' was the most common word in porn titles (BJC, 2020). 'Teen' actors are frequently depicted as youthful and childlike, playing roles that accentuate their youthfulness, such as schoolgirls, little sisters or cheerleaders being coerced into sexual encounters with older babysitters, coaches or family members.
- **Hentai/anime porn (animated content):** Of note, cartoon content is among the most searched for and viewed content on mainstream sites. In animated content, the female characters often possess child-like features, with the exception of exaggerated breasts and enlarged genitalia. Additionally, these depictions frequently involve explicit and violent sexual encounters, often with 'monster' male characters. A prevalent theme within the genre includes grotesque creatures engaging in non-consensual acts with female characters, commonly depicted through the use of oversized phallic appendages or 'tentacles'. Children are disproportionately exposed to 'non-photographic' forms of pornography (BBFC, 2022).

- **Stereotypical gender depictions:** Men are typically portrayed as aggressive and dominant in porn, while women are commonly depicted as submissive and objects of male pleasure. Aggressive male peer dynamics are also common, such as groups of men engaging in rough or forced sex with one woman.

2.2 CHILD SEXUAL ABUSE MATERIAL (CSAM) AND OBJECTIONABLE CONTENT

2.2.1 CSAM

Digital platforms have amplified the spread of CSAM, which encompasses any depiction – real or AI – of a child nude or engaged in sexual acts.

Offenders exploit children through grooming, sexual abuse, or financial incentives to produce and distribute CSAM online. Social media, messaging apps and gaming platforms not only facilitate CSAM dissemination but also enable grooming, live-streamed abuse, and offender collaboration (UK Government, 2021; UNICEF Innocenti, 2023).

Globally, 1 in 5 children faces online solicitation, a rate that has tripled since 2021 (ECPAT, 2023; Internet Watch Foundation [IWF], 2023). CSAM volume has surged by 87% over the past five years (WeProtect Global Alliance, 2024). In 2023, the CyberTipline operated by the US National Center for Missing and Exploited Children (2024) recorded 36.2 million reports of suspected online child sexual exploitation, with online enticement reports rising over 300% from 2021 to 2023.

In New Zealand, online child sexual exploitation reports have nearly quadrupled over the past five years (New Zealand Police, 2024). Globally, self-generated sexual imagery among 7-10-year-olds increased by 360% between 2020 and 2022 (IWF, 2023). Data indicates that 55% of victims are contacted by traffickers on mainstream social media platforms (Insoll et al., 2024; Protect Children, 2024). Grooming on gaming platforms can escalate within 19 seconds, averaging 45 minutes per incident (WeProtect Global Alliance, 2024). Once produced, CSAM perpetuates victimisation through ongoing online circulation (Christenson et al., 2020).

2.2.2 AI-generated CSAM: 'Nudify' apps and animated content

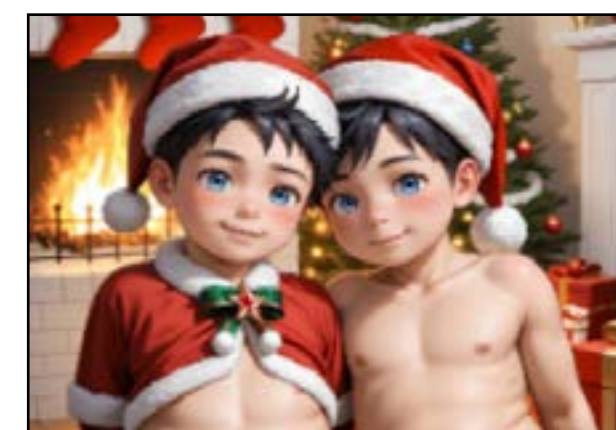
Recent advancements in AI have led to the emergence of AI-generated CSAM, particularly deepfakes.

Offenders use AI tools to 'nudify' or manipulate legitimate images of children, potentially sourced from social media, into sexually explicit content. By fine-tuning AI models with specific prompts, clothed images are transformed into abusive material, amplifying the scale and accessibility of CSAM (WeProtect Global Alliance, 2024).

Nudify apps enable the creation of fake nude images, disproportionately affecting young girls. These images, often generated by peers, are circulated in schools and communities, causing significant harm. In 2023, reports of such incidents among teens rose by 25% globally (Thorn, 2024).

Animated CSAM, including genres like lolicon, toddlercon, and shotacon, depicts fictional child characters in sexually suggestive or explicit scenarios. This material is often shared on message boards, with access to more explicit content may require paid accounts.

Research indicates children aged 6-17-years-old are more likely than adults to encounter such material, which may normalise abusive relationships (BBFC, 2022) or normalise the sexualisation of children. In 2024, Gen Z was 193% more likely to view hentai on Pornhub, a 100% increase from 2023 (PornHub, 2024).



(Images obtained from www.deviantart.com/tag/lolifetish, 2025)

Hentai and 'Twink' (male characters with slim, youthful builds) were the top categories on Pornhub Gay, highlighting their popularity. A former offender noted, "Consuming lolicon and shotacon manga lowers barriers to viewing children as sexual targets" (Kato, 2024).

"Hentai, we show, encourages adults to see minors, especially girls, as legitimate targets of sexual violence."

(Dines & Sanchez, 2023)

2.2.3 Dark web and encrypted platforms

The dark web and encrypted messaging apps have become key vectors for CSAM distribution, offering anonymity to offenders. In 2024, INTERPOL reported a 65% increase in CSAM-related cases linked to dark web marketplaces compared to 2020. Encrypted platforms, such as Telegram and Signal, are increasingly exploited for sharing abusive material, with groups forming to exchange content or coordinate live-streamed abuse (Europol, 2024). In New Zealand, police noted a 40% rise in CSAM cases tied to encrypted apps between 2022 and 2024 (New Zealand Police, 2024). These platforms complicate law enforcement efforts due to end-to-end encryption and jurisdictional challenges.



Source: Bing search “Young rape porn” (2025).

2.3 BESTIALITY AND RAPE-RELATED CONTENT

2.3.1 Bestiality

Bestiality content remains widely accessible via major search engines. A 2024 search on bing.com yielded 889,000 image results for 'bestiality' and 2.3 million for 'bestiality porn', highlighting the ease of access to such material (Bing, 2024).

2.3.2 Rape-related content

Search engines have faced scrutiny for rape-related content accessibility. In 2021, Google inadvertently suppressed 'rape porn' search results due to a machine learning adjustment, though it remains unclear if this was intentional or not, and if such content is filtered or demoted. Bing has since modified 'rape porn' results following advocacy efforts, but terms like 'forced porn' and 'rape young porn' remain easily searchable (Makes Sense, 2024).

Offenders currently embed rape-related videos within non-sexual image search results, complicating detection.

2.4 ONLINE READING, WRITING, AND STORY-SHARING COMMUNITIES

These increasingly popular platforms offer young people opportunities to read, write, share and explore stories as part of an online community where they can interact with peers through comments, likes, feedback and forums.

Common platforms used by young people include Wattpad (90 million monthly users), AO3, Radish Fiction, Smashwords, Asianfanfics, Fanfiction.net, and Tik Tok’s book site Book Tok (#BookTok has had over 181.7 billion views). The platforms are marketed to teens (13+) and young adults, but are freely accessible to children and tweens, and lack formal age verification measures. While they offer valuable opportunities for reading, they also host a growing range of unmoderated and user-generated adult sexual fantasy including 'Dark Romance'. This subgenre is centred around disturbing and taboo sexual themes, such as rape, sexual horror, manipulation, toxic relationships, obsession, coercion, domination and abuse. Some Dark Romance novels can also be explored via virtual reality platforms in immersive virtual settings through avatars.

Anecdotal feedback from youth in Aotearoa suggest these platforms are increasingly being accessed by youth of all ages, often by young readers aged 12-14 years, with genres such as Dark Romance increasingly popular.

2.5 GENERATIVE AI AND AI-GENERATED PLATFORMS

Generative artificial intelligence (GenAI) refers to artificial intelligence (AI) systems that can create content derived from existing datasets.

This technology is being rapidly integrated into all parts of society, particularly with the introduction of platforms like ChatGPT by OpenAI. Launched in late 2022, ChatGPT quickly became the fastest-growing consumer application in history, amassing around 100 million monthly active users by January 2023 (UBS Chief Investment Office, 2024).

Young people have embraced GenAI for various purposes, including homework assistance, socialising with chatbots, and creating artwork. According to a report by Common Sense Media, 70% of teenagers in the United States have used GenAI tools, with over half engaging with AI text generators and chatbots. The rapid adoption of these technologies is mirrored in a UK report, which found that 4 in 5 teenagers utilised GenAI tools, with usage increasing from 50% in 2023 to 80% in 2024 (Ofcom, 2024).

GenAI encompasses a variety of AI platforms, including chatbots, image generators, and virtual companions.

The most notable examples include ChatGPT, Microsoft Copilot, Character.AI and Replika, among many others. These platforms are designed to engage users in diverse ways, from content generation to creating synthetic relationships.

GenAI may pose unique risks to children and youth, whose cognitive processes are developing. Research indicates that a substantial portion of interactions with GenAI involve sexual content. The dataset WildChat is a corpus of over 1 million human - ChatGPT interaction logs, and analysis shows that sexual role play constituted 12% of user interactions (Zhao et al., 2024). Despite OpenAI's guidelines prohibiting sexual content involving minors, users have been able to manipulate the system to bypass safety filters, raising concerns about the exposure of young users to sexual AI conversations (Zhao et al., 2024).

An emerging trend in GenAI is the creation of synthetic relationships, where young users engage with chatbots for companionship or fantasy. Platforms like Character.AI and Replika are at the forefront of this trend, allowing users to interact with AI in increasingly intimate ways. Character.AI, for instance, targets users aged 13-25 and has seen significant growth, with 1.7 million installs in its first week after it launched in 2021 and 20 million active users by mid-2024 (Weam, 2024).

The average session time on Character.AI is reported to be 34 minutes, with users spending an average of 2 hours per day on the platform. However, the lack of age verification and content moderation raises significant concerns about the potential exposure of young users to harmful sexual AI relationships (eSafety Australia, 2025).

In addition to conversational AI, GenAI technologies such as Stable Diffusion enable the creation of photorealistic pornographic images and videos. A survey commissioned by Snapchat revealed that 24% of teens across six countries had encountered AI-generated sexual content (TRG, 2024). Furthermore, in 2023 Thorn's annual Youth Perspectives on Online Safety survey indicated that 11% of respondents believed their peers had used AI to create nude images (Thorn, 2024).

As GenAI continues to evolve, new challenges are emerging. Some AI platforms, such as Grok 3, are moving towards less moderation, making it easier for users to access unfiltered content without the need for 'jailbreaking' (attempts to bypass the safety measures and ethical guidelines built into AI models). This trend raises urgent questions about the safety and wellbeing of young users using GenAI in an increasingly complex digital sexual landscape.

There is a dangerous lack of accountability over language model training data and content moderation, which poses significant risks. OpenAI's announcement in mid-2024 that it would allow developers to create NSFW content, albeit not pornography, further complicates the issue.

The accessibility of GenAI tools is a double-edged sword: The potential for huge increases in productivity comes with the perils of child sexual exploitation. The absence of age-appropriate design, lack of age verification, and the freely available services make these tools easily accessible to young users.

An emerging trend in GenAI is the creation of synthetic relationships, where young users engage with chatbots for companionship or fantasy.

2.6 EXTENDED REALITY PLATFORMS

Extended reality (XR) technologies provide immersive experiences that blend the physical and digital worlds. They have gained popularity in recent decades, particularly in social gaming and adult entertainment.

Extended reality technologies can be categorised into three main types based on immersion levels:

- **Virtual reality (VR):** Offers complete immersion in a 3D environment, often using headsets.
- **Augmented reality (AR):** Overlays digital content onto the physical world, enhancing real-life experiences.
- **Mixed reality (MR):** Combines elements of both VR and AR, allowing interaction with both physical and digital objects.

The immersive nature of XR creates a unique environment for sexual experiences, with users able to engage in virtual sexual acts through customisable avatars. Some platforms explicitly cater to adult content, offering pre-programmed sexual scenarios or allowing users to create their own experiences.

Extended reality offers new adult consensual sexual experiences. However, there are blurred lines when physical and virtual worlds are fused. There are ethical and legal considerations around consent, age verification and the potential for exploitation or harassment in virtual spaces that require regulation and monitoring by platform creators (Pettifer et al., 2020).

Extended reality technologies have the potential to create human trauma not experienced through any other technology because of the ability to create immersive sexual experiences (Thorn & WeProtect Global Alliance, 2024).

Global research indicates that a substantial portion of young users encounter sexual content in these spaces.

A US survey of young people between 13 and 17 years old found 33% owned a VR headset, with the majority owning either the Meta Quest/Quest Pro or PlayStation VR. Youth reported using a variety of apps such as VRChat, Rec Room, Horizon Worlds, AltspaceVR, Couch, Horizon Venues, BeanVR, NeosVR, VTime XR and SanSar, among others. Nearly 21% had encountered unwanted violent or sexual content and 18% had experienced grooming or predatory behaviour. Almost 19% of young VR users experienced sexual harassment (Hinduja & Patchin, 2024).

Research from the Center for Countering Digital Hate highlights the prevalence of abusive behaviour in XR environments, with users exposed to harassment every 7 minutes in platforms like VRChat. Fairplay found similar results with Horizon Worlds, a platform where children under 13 make up a substantial part of the user base. Every time a user logs on, they face the threat of sexual predators, financial harm, bullying and harassment.

The rapid adoption of XR technologies has been fuelled by improvements in mobile augmented reality, internet capabilities (e.g., fibre, 5G) and the decreasing costs of VR headsets. As XR platforms become more accessible, the potential for young people to encounter sexual content increases. Indications of youth exposure have come from public attention drawn to some of these risks to children in VR. For instance, journalists going 'undercover' have found that children under 10 have been approached by adults in VR social spaces, exposing them to pornographic and violent content (Pettifer et al., 2022).

Sexual content is a prominent feature in many XR environments, with a significant market for adult consensual experiences using technology such as motion tracking and haptics (mimicking the sense of touch). Guggisberg (2024) highlights the growing threat of VR grooming and emphasises the need for parental awareness, as well as for digital literacy education, broader societal changes, and regulation.

The blurred lines between childlike aesthetics and adult themes in XR games can create confusion for both parents and children. Many VR games feature cartoonish designs that may appear child-friendly, yet they might include activities that are not age-appropriate. This raises ethical concerns regarding consent and age verification, and makes the VR environment easy for predators to exploit or harass victims (Pettifer et al., 2022).

New Zealand research on youth experiences with XR/VR safety and exposure to online sexual experiences is limited. Content moderation technology for XR technologies is still in the early stages of development - the animated nature of the metaverse makes traditional content moderation technology ineffective.

While the cost of entry-level VR headsets has decreased, affordability remains a barrier for many young people. The introduction of Apple Vision OS and Apple VR headsets has raised this barrier with premium prices. Current research shows only 14% of VR headset owners use them weekly, indicating that, while ownership is growing, regular engagement may be limited (Piper Sandler, 2023). Over the next couple of years XR technologies will converge with social media platforms and AI, such as Snapchat and Character.AI, which are planning to deliver VR features. Consequently, higher youth uptakes and engagement are expected in the future.



2.7 SOCIAL MEDIA AND MESSAGING APPS/PLATFORMS

While YouTube qualifies as a social media platform due to its user-generated content, its classification presents challenges because it is more commonly used for entertainment, news or educational purposes rather than for the primary social connection typically associated with mainstream social media.

Every year, minors report using a wide range of platforms, regardless of these platforms' intended audience or age-related policies. In 2023, the platforms with the highest daily usage rates were YouTube (83%), TikTok (64%), Snapchat (48%), Facebook (47%) and Instagram (45%) (Thorn, 2024). Minors continued to report using applications designed for adult users (18+) to "escape" and foster relationships, romantic and otherwise. Loneliness appears to be a risk factor for engaging problematically online (Burrus et al., 2024; Sun & Zhang, 2021).

The top platforms minors were most likely to indicate they had experienced an online sexual interaction were Omegle (36%), Kik (23%), Snapchat (23%), Telegram (22%), Instagram (20%) (Thorn, 2024).

In New Zealand, 23% of people aged 18 and over surveyed in 2021 reported that in the year prior they had "been exposed to offensive and unwanted content on social media or content sharing platforms" (Netsafe, 2021).

Nadia Maxwell, a New Zealand documentarian, discovered that within just 22 minutes of creating a child account on TikTok, the platform was showing suicide-related content (Leask, 2024), contradicting claims made by social media companies about their safety measures.

As in past years, social media was reported by nearly a third of adolescents as the most authentic media space (31%). Given the sexualised content on these platforms, which is often aggressive and misogynistic, young people perceiving them as authentic is concerning. (Burrus et al., 2024, World Health Organization, 2024).

According to the US National Center for Missing and Exploited Children (NCMEC, 2024), Meta reported more than 20 million incidents of people sharing child sexual abuse imagery on Facebook and Messenger in 2022 (NCMEC, 2023). It will be more difficult to attain data as accurate as these and intervene after Meta introduced encrypted messaging in 2023-2024 (NCMEC, 2023).

Social media now acts as the 'digital storefront' for the porn and sex industry, with performers and companies using it as platforms to advertise less explicit content and draw viewers onto their platforms (e.g., OnlyFans).

The impacts and risks associated with engagement with sexual content through social media and messaging platforms are far-reaching. These include, but are not limited to, exposure to harmful content, online harassment, exclusion, doxxing, technology-facilitated sexual violence, exposure to predators, long-term reduced face-to-face relationship skills, and the normalisation of harmful sexual attitudes and behaviours through echo chambers, misinformation, and limited critical thinking. These are detailed in Section 3.1 below.

“One-in-eight 13-to-15-year-olds had experienced an unwanted sexual advance on Instagram within a week.”

(Arturo Béjar, former Meta senior staff member, 2023 US Congress testimony)

2.8 MAINSTREAM STREAMING SERVICES

Mainstream streaming services are digital platforms that provide on-demand access to TV shows, movies, documentaries, and other video or audio content, often through subscription-based models.

These services have become a dominant form of media consumption, offering convenience, personalised recommendations, and vast content libraries. The most popular platforms, such as Netflix, YouTube, Disney+, Prime Video (Amazon) and Spotify, have hundreds of millions of users worldwide.

Mainstream platforms are now developing gaming functionality and promoting sexual-themed games rated 17+. See image on following page for Netflix game advertisement.

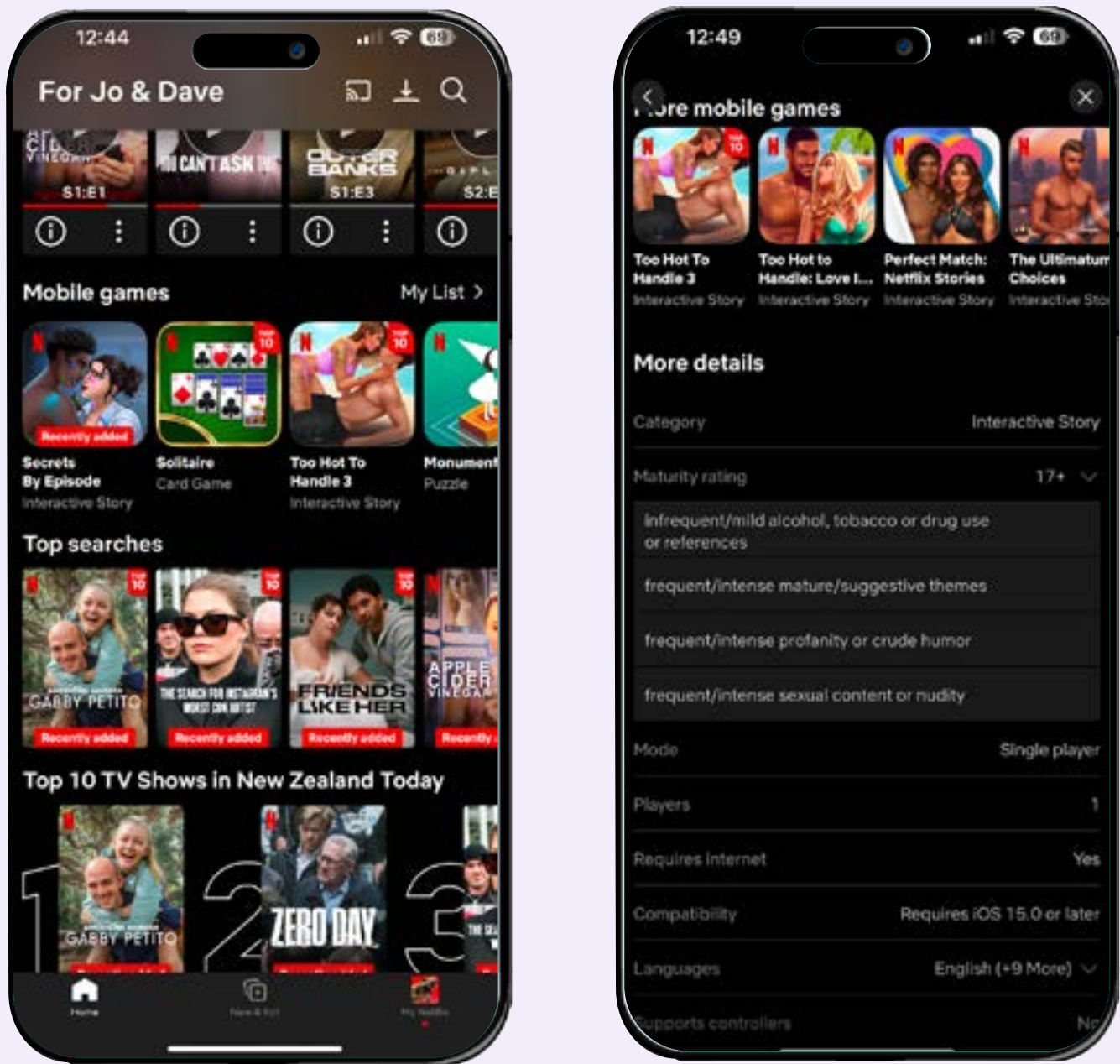
Adolescent females exhibit a preference for series such as Euphoria, Outer Banks, Gossip Girl (revised series), Monsters: Lyle & Erik, Shameless, Love Island and Heartstopper. In contrast, adolescent males predominantly engage with video gaming and YouTube content, which are addressed in separate sections of this report. Several of the aforementioned series feature highly sexualised content, with certain narratives incorporating themes of incest and depictions of illegal sexual acts.

This analysis focuses exclusively on the sexual messaging within these programs, omitting exploration of other themes that may yield positive influences.

Two examples illustrating their content and messaging are provided below:

Cruel Intentions (2024, Prime Video): Based around university-age students in sororities. Episode 1 includes a video recording of a sexual encounter in which consent is not shown.

A stepmother intimately touches her stepson's inner thigh. A stepbrother and sister are nude in front of each other and have a sexual exchange: "I'll give you whatever you want. What you've always wanted, me, for up to an hour." These characters call each other brother and sister.



Euphoria (2019, HBO): Based around a diverse range of high school students. One character's storyline involves a non-consensual recording during sex, which leads her to becoming a camgirl as a means of reclaiming control over her sexuality. The narrative seems to frame this as empowering. Legally, this constitutes CSAM, though the show does not label it as such. Another character engages in in-person sexual encounters with older men she meets online, some of which involve rough sex. These encounters are filmed non-consensually and used as pornography. Legally, this is also CSAM, yet the show does not address it.

“Euphoria often feels more like an instructional tutorial or a road map, one that sensationalizes its subject matter while neglecting to fully disclaim its risks and hazards ... Teenagers may have already been overexposed and over-adultified and already participating in the kinds of things Euphoria depicts – but the last thing we needed was a vehicle to further romanticize our self-destructiveness.”

(Getachew, 2022)



2.9 DATING APPS

Mobile dating apps and websites are an increasingly popular and socially acceptable way of meeting people. A number of apps, such as Bumble, Tinder and Grindr, offer spaces for adults to connect and engage in online flirting, dating, romance and sexual experiences.

In an Australian study, Wolbers and Dowling (2024) examined how certain online behaviours may increase vulnerability to sexual violence via dating apps. The researchers determined the use of dating apps is high-risk even for adults, and a very high percentage of users are exposed to dating app-facilitated sexual violence (DAFSV). DAFSV encompasses various risks, including unwanted sexual harassment, unsolicited explicit photos, and gender-based aggression. Wolbers and Dowling (2024) found that over two-thirds (69%) of mobile dating app users had faced online sexual harassment from individuals they met through these platforms. Additionally, nearly half of respondents reported continued contact from someone after expressing disinterest, and a similar percentage received unwanted sexually explicit messages.

The pressure to engage in sexual activities is also prevalent, with 38% of users feeling pressured to send sexual messages, 38% pressured to share sexual images or videos, and 35% pressured to meet someone in person

against their will (Wolbers & Dowling, 2024). These statistics underscore the urgent need for protective mechanisms on dating platforms to safeguard users from DAFSV and prevent perpetrators from targeting others.

Thorn (2023), meanwhile, found that children are accessing adult dating platforms in significant numbers, with 19% of US minors reporting using adult dating apps like Tinder, Grindr, Hinge and Bumble, with boys aged 9-12 years notably participating.

Apps like Tinder, Bumble and Grindr are designed for adults, however numerous similar platforms are available for children as young as 12 years old and are marketed as 'friendship apps'. Adult dating apps, such as Tinder and Grindr, require users to be 17 or older. Many friendship apps, including Wizz, Wink, Hoop, Tiya and ItsMe are presented as a way to 'make friends' and are designed for children to connect with strangers online.

A US meta-analysis titled "Teen Tinder? An Analysis of App-store Reviews of Adolescent 'Friendship' Apps" (Rosenthal et al., 2022) analysed 2,500 reviews of various friendship apps and found that 22% referenced inappropriate content.

Specifically, over 7% mentioned sexual content, 4% referenced dating, and over 9% reported scams. Reviewers referred to the Wizz app in some instances as "kid tinder", while the Hoop app was described as having "so many pedophiles". The findings highlight the alarming presence of predatory behaviour, a lack of moderation, and a lack of regulation by app stores, which poses significant risks to children who may be manipulated into engaging with explicit content, sharing sensitive information, and online grooming (Rosenthal et al., 2022).

2.10 PLATFORMS FOR SELF-GENERATED SEXUAL CONTENT

These platforms facilitate the sale of sexual content through subscription-based services, including live webcam shows, video sales, and the exchange of nudes or other intimate content. They can also offer opportunities to engage in transactional sexual relationships offered by 'sugar daddy' and 'sugar mummy' sites.

This industry has experienced substantial growth in the last few years, driven by increasing demand and the continuous emergence of new platforms. In early 2024, a Google search for 'selling nudes' yielded approximately 1.6 billion results, highlighting the scale of the market. Popular sites include OnlyFans, ManyVids, Fansly, JustForFans and Chaturbate. Among these, OnlyFans is the market leader, with approximately 468 million visits per month in December 2024; an estimated 70% of its users are under 34 years old (Statista, 2025).

Selling sexual content is a rapidly expanding and attractive arena among young people in Aotearoa, and while most platforms claim to have strict R18 age verification, some don't, increasing the risk of young people creating and/or purchasing sexual content.

A 2024 US study found 15% of teens aged 13-17 and 4% of children aged 9-12 reported using OnlyFans (Thorne, 2023). Accessibility is amplified by the ease with which content creators leverage mainstream platforms like Instagram and TikTok, using trends, hashtags and 'teasers' to gain viewers and drive traffic to their adult sites via bio links. This has also heightened the risk of unintentionally accessing explicit sexual content via mainstream social media.

2.11 CHILDREN'S SITES AND GAMING

Hundreds of millions of children enjoy online gaming daily. Some games enable players to create their own VR, with many games involving user interaction, enabling users to play with both friends and strangers worldwide.

Research by the eSafety Commissioner in Australia found that while most children have positive experiences through social contact and learning something new while playing online games, a significant number have negative experiences, with around half of teen gamers exposed to harmful experiences.

Three of the top 5 platforms used by children in the United States are online games: Roblox, Minecraft, and Fortnite (Thorn, 2023).

- **Roblox:** A game-creation platform with 79.5 million daily active users. It allows users to design and play games created by others. Its design is heavily influenced by the metaverse. It has been criticised for inadequate content moderation, leading to the proliferation of inappropriate content, including sexual exploitation (Zapal, 2023). Roblox has no age restrictions on chatrooms, and researchers found that 21% of its users are under the age of 9, highlighting the vulnerability of its young audience (Hindenburg Research, 2024).
- **Minecraft:** With 166 million monthly players and over 600 million copies sold, Minecraft appeals to both children and adults. Its popularity surged during the COVID-19 pandemic. Concerns remain regarding the exposure of young players to inappropriate content.
- **Fortnite:** A popular battle royale game where players compete to be the last one standing. It allows players to compete and customise characters. Fortnite has 110 million monthly active users, hosts events, and utilises an in-game currency known as 'V-Bucks'.

Some games and online platforms connect players to spaces that are decentralised and not monitored or controlled by a central authority. This means there are few rules or safety checks in place.

Apps like Discord and Telegram are popular for chatting while gaming, but some of their groups (or 'servers') also share adult content labelled as R18. Even though it's marked for adults, there's no real regulation – anyone can join and see the content, regardless of their age.

Examples of emerging trends and developments in gaming:

- **Grand Theft Auto** is a game series that is rated for mature audiences but has become increasingly accessible to young people. It features hypersexualised content that raises alarms about its influence on youth.
- **Sexual content in games on the Steam store is concerning.** Reports indicate that platforms like Steam, which offers over 73,000 games, allow objectionable content to be accessible to minors. In one case, a pornographic game containing rape simulation and incest titled No Mercy was rated 12+ was removed from the store, raising questions about the effectiveness of moderation on such platforms.
- **Groups like 764** have been identified as targeting young people through sextortion and grooming, indicating a growing trend of organised exploitation within gaming communities.



3

What are the Risks and Harms?

The digital landscape poses increasing risks for youth, including image-based abuse, online grooming, harassment, coercion, and early exposure to CSAM.

Pornography further reinforces harmful norms, raising the risk of sexual violence, especially among vulnerable youth. Outside the scope of this report but of concern is growing research around how increased online engagement, as opposed to in-person interactions, reduces opportunities to develop crucial social skills like listening and empathy, which are often shaped by face-to-face communication.

3.1 TECHNOLOGY-FACILITATED SEXUAL VIOLENCE

Technology-facilitated sexual violence encompasses various forms of abuse facilitated by technology, including image-based abuse, online grooming, sexual harassment, and coercion.

Technology-facilitated sexual violence behaviour is usually motivated by the desire for sexual gratification or harassment, but it can also have a financial motive, such as sextortion.

The impact of TFSV varies depending on factors like age, neurodiversity, trauma history, and parental mediation. Thorn (2023) reported that 59% of US minors had had a potentially harmful online experience, and 35% had had an online sexual interaction.

3.1.1 Image-based abuse

Image-based abuse is non-consensual sharing of images or videos by perpetrators for purposes such as sextortion, revenge porn, harassment, and coercive control.

AI deepfakes have made IBA more complex, as detailed below.

While data on the prevalence of IBA is limited, Henry et al. (2023) examined the lived experiences of victim-survivors of IBA in Aotearoa New Zealand with respondents aged 16–64 years. Thirty-five per cent of respondents reported that someone had taken a nude or sexual image of them without their consent, and 22% had had this content shared.

Māori respondents (48%) were more likely than non-Māori (38%) to have experienced IBA, and LGBTQIA+ respondents under 39 years of age were significantly more likely to report experiencing IBA than their heterosexual or older counterparts.

Bloxham et al. (2024) found the leading reasons young people participate and are coerced to 'self-produce' are solicitation, peer sexting, viral challenges, sextortion, and financial coercion. Youth services in Aotearoa note that while sharing nudes is common, many are consensual and go no further than the intended recipient. However, if they do, the consequences are more harmful for young women. During the 2024 Otago University Orientation Week, Netsafe (2024) surveyed hundreds of students and found that 54% had had photos shared online without permission.

Image-based abuse can be a form of retaliation that is colloquially referred to as 'revenge porn'. This form of abuse often occurs in the context of relationship breakdowns. For the victim, it can lead to severe reputational damage and psychological harm.

3.1.2 Sextortion

A form of online blackmail involving coercing individuals, often young people, to produce and share sexually explicit images or videos. Offenders then threaten to release the shared images unless their demands are met.

Predominantly, perpetrators connect with victims on popular social media platforms before moving conversations to messaging apps with image-sharing capabilities and end-to-end encryption, which include Snapchat, Instagram, WhatsApp, Facebook Messenger, and iMessage. A small number of sextortion cases are perpetrated by partners or peers.

In recent Australian research, 1 in 10 adolescents said that someone had sexually extorted them for money or more intimate material (Wolbers et al., 2025). Children as young as 8-years-old had been sextorted, and 65% of sexually extorted adolescents were extorted by someone they met online but never in person. In a small number of cases the victim was coerced into offending themselves, sometimes through sexually deviant behaviour or bestiality.

Multiple reports indicate a significant rise in sextortion cases. In 2023, the National Center for Missing and Exploited Children (2024) received 26,718 reports of financial sextortion – up from 10,731 reports in 2022. In New Zealand, Netsafe (2023) received 1,707 reports of sextortion in the year ended 30 June 2023, a 237% increase on the same period the previous year.

3.1.3 AI deepfakes

AI deepfakes are fake realistic looking non-consensual intimate images created using GenAI.

A 2023 study by the US cybersecurity firm Security Hero found that 98% of all deepfake videos were pornography, and 99% of the subjects were women.

The resulting harm from AI deepfakes causes immense distress for the individuals whose images are used and shared without their consent, even if it becomes clear the content is fake. The potential for causing humiliation, shame, harassment, intimidation, or being used in sexual extortion is just as likely whether the content is genuine or synthetic.

Deepfakes only require one image to be manipulated to create convincing content that could lead to harassment and extortion. The rapid advancement of AI technology raises concerns about the potential for viral widespread misuse in schools and by cybercriminals. In addition, the proliferation of fake CSAM is causing wide concern, stretching law enforcement efforts and making victim identification harder for police.

3.1.4 Online grooming

Online grooming is when adults or older youth use online communication to draw youth into sexual relationships.

Offenders often use social media and messaging platforms to build trust with children, making them vulnerable to exploitation. The prevalence of grooming is alarming, with at least 1 in 10 young people experiencing online grooming (Schittenhelm et al., 2024) and two-thirds of youth happy to interact with people they don't know, unaware of the risks involved in sharing personal information (Third et al., 2024).

“It takes only 8 minutes for a predator to bond with a child.”

(International Centre for Missing and Exploited Children, 2024)

Perpetrators use a range of tactics, including targeting, building trust, testing boundaries, isolating, exploiting, and blackmailing to undermine protection factors (Masters, 2023). Survivors can suffer very high levels of psychological distress (Finkelhor et al., 2024).

While some platforms do have moderation, perpetrators often shift victims to less-monitored spaces. In 55% of reported cases, aggressors quickly reconnected by creating new accounts or switching platforms (Thorn, 2023).

3.1.5 Sexual harassment and bullying

Digital platforms have become venues for sexual harassment, where individuals face unwanted sexual advances, explicit language, and intimidation.

Sexual rumours and manipulative tactics are common, with perpetrators using false promises of relationships to coerce victims into sharing explicit content.

Online behaviours can be reported as bullying, but they do in fact meet the threshold for sexual harassment. This is illustrated by findings from Barker-Clarke et al. (2023), who note that ‘the majority of dick pics are unsolicited and often make young female recipients feel unsafe’.

3.1.6 Synthetic sexual abuse

Emerging conversational AI platforms such as Character.AI have shown that perpetrators can also now be synthetic, without any financial, sexual or human motive.

A lawsuit was filed against Character.AI in 2024 after a 14-year-old boy from Florida, Sewell Setzer, committed suicide. The co-founder of the US Humane Technology Coalition Tristan Harris noted that “Character.AI acted human with very overt ways of being sexual with Sewell and asking him to join her on the other side, ultimately leading to his suicide” (Kilmeade, 2024).

Synthetic sexual abuse is a new and concerning risk. Discussion on Reddit forums alongside reports from community-based services identifies addictive AI girlfriends and AI boyfriends on platforms such as Character.AI as a growing threat due to the pervasive and persuasive nature of the apps involved, which market and target the developing of intimacy with young people.

Currently there is limited research due to the rapid emergence of this technology. Further research is needed to explore this recent innovation, yet challenges are presented by the pace of change.

In the future, GenAI and other emerging technologies could allow perpetrators to scale TFSV harm by using AI automation to amplify risks and harms.

3.2 EXPOSURE TO CSAM & CHANGING SEXUAL NORMS

“Every five seconds, a child somewhere is exposed to harmful online content. The responsibility to act falls on governments, tech companies, and global civil society alike.”

(WeProtect Global Alliance Statement, 2024)

This subsection describes the prevalence, harms, and emerging issues surrounding CSAM, including hentai and AI-generated content. CSAM viewership can be distinct from paedophilia (a psychological condition involving sexual attraction to children) and physical child sexual abuse. These distinctions are critical, as research often does not specify whether CSAM involves real or AI-generated content or whether the offending stems from paedophilia or impulsive/opportunistic behaviours.

The growth and exposure to CSAM has dramatically increased because of online child exploitation.

New Zealand Police, the Department of Internal Affairs (DIA) and Customs Service issued a joint statement in 2024 urging parents to prioritise the online safety of their children (New Zealand Police, 2024). This is due to the rapid and alarming rise in self-generated CSAM. Globally there has been a 1,816% increase in self-generated CSAM featuring 7-10-year-olds since 2019 (Internet Watch Foundation [IWF], 2023).

“The majority of objectionable material that New Zealand agencies deal with show real children being harmed through often-horrific sexual abuse.”

(New Zealand Police, 2024)

The UK National Crime Agency (2023) estimated that 1.3-1.6% of the adult population poses some degree of sexual risk to children, noting that “a real increase caused by the radicalising effect of the internet, where the widespread availability of videos and images of children being abused and raped, and groups sharing and discussing the images, has normalised such behaviours”. While these data refer to adults, young people also report seeing this content and being able to access these groups.

3.2.1 Prevalence of exposure

Exposure to CSAM is a significant concern, particularly among young people. Unfortunately, New Zealand-specific prevalence data on youth engagement with CSAM or rape content are absent.

Global research provides the following insights:

- Between 9 and 14% of 16-24-year-olds have been exposed to illegal content, including CSAM, with 11% encountering it weekly, 10% 2-3 days a week, and 7% daily.
- Social media accounts for 35% of encounters with unsafe, age-restricted or illegal content among teens (Verifymy, 2024).
- Among individuals seeking CSAM, 70% first saw it before age 18, with 40% under 13 at first exposure. Over 50% of these individuals were not actively seeking CSAM when first exposed (IWF, 2022, 2023).

3.2.2. Vulnerable groups and risk factors

Certain groups are more vulnerable to CSAM exposure. Unemployed individuals not seeking work, students, and children who witness aggression are at higher risk (IWF, 2022).

Research shows children experiencing neglect are 2.7 times more likely to engage in risky online behaviours, increasing their exploitation risk (Emery et al., 2024).

Other facilitators include:

- adverse childhood experiences, which heighten vulnerability to harmful online content
- substance use, which lowers inhibitions and increases risk-taking
- desensitisation to adult pornography, which may escalate to CSAM consumption (Insoll et al., 2024; Project2Know, 2025).

3.2.3 Harms and impacts

CSAM exposure has profound negative effects on young people and survivors.

Key findings of recent research international studies include:

- 69% of 16-19-year-olds exposed to CSAM report a negative impact, with 44% citing direct mental health consequences (IWF, 2022).
- Exposure can retraumatise survivors of sexual abuse, intensifying shame, fear and helplessness, and hindering recovery (APA, 2021., AIFS, 2020).
- Early exposure to CSAM is an adverse childhood experience linked to trauma-related disorders like acute stress disorder and post-traumatic stress disorder, which increase the likelihood of violent offending in adolescence (Kessler et al., 2007; Keyes et al., 2012; Peltonen et al., 2020).
- Among CSAM offenders, 58% fear their viewing may lead to in-person abuse, 50% report self-harm thoughts or suicide attempts related to their behaviour, and many express shame and a desire to stop (IWF, 2023).
- 42% of CSAM users have sought direct contact with children online after viewing such material (IWF, 2023).

- Young people's responses to CSAM vary: 36% report it to the website, 38% close the site, 35% ignore it, 11% inform parents, and only 9% report to authorities (IWF, 2022).

3.2.4 Offender motivations and behaviours

While sexual interest in children is a known driver, CSAM offending is also motivated by emotional regulation difficulties, high sex drive, and sensation-seeking tendencies (Insoll et al., 2024; Project 2Know, 2025).

AI-generated CSAM, while not involving real children, poses similar risks by eroticising minors and desensitising consumers to child sexual abuse. In 2024, Derek Ray-Hill, interim CEO of IWF, stated:

People can be under no illusion that AI generated child sexual abuse material causes horrific harm, not only to those who might see it but to those survivors who are repeatedly victimised every time images and videos of their abuse are mercilessly exploited for the twisted enjoyment of predators online.

To create the level of sophistication seen in the AI imagery, the software used has also had to be trained on existing sexual abuse images and videos of real child victims shared and distributed on the internet (IWF, 2024).

Such content reinforces harmful fantasies and may increase demand for CSAM.

Young people in New Zealand report disturbing and confusing experiences with accidental exposure to CSAM. Feedback from youth helplines suggests many youth are reluctant to report these experiences or speak to a trusted adult, for fear of getting into trouble. Confusion is particularly high around AI-generated CSAM and animated genres like lolicon and shotacon (see Section 2.2), with some young people believing it may be acceptable to view because “it’s not real”. This uncertainty and fear mean harmful exposures are often left unreported and unaddressed, placing youth at risk.

3.3 SHIFTS IN SEXUAL ATTITUDES, BELIEFS AND BEHAVIOURS

Studies reveal that the prevalence of sexual aggression, degrading portrayals of women, misogyny, rigid gender roles, sexism, and the normalisation of violence within mainstream porn culture and content can contribute to the development of harmful sexual attitudes, beliefs and behaviours

(Upton et al., 2020; Pathmendra et al., 2023; Lim et al., 2016; Mori, 2023; Donevan and Mattebo, 2017; Rodenhizer and Edwards, 2019; Wright et al., 2016; Waterman et al., 2022; Ybarra et al., 2018).

While the nature and strength of this connection vary across the literature, evidence consistently highlights its influence.

When considering this, it is important to recognise the unique vulnerability of children and adolescents to online porn. As we have seen, most first encounter porn around the ages of 12-13, a critical stage in their sexual development. For many, porn serves as a primary source of sexual education.

However, many youth have limited life experience or sexual

knowledge to contextualise what they see, particularly regarding what is realistic, safe or mutually acceptable, making them more susceptible to perceiving some of the problematic messages in porn as ‘normal’. Additionally, they generally view porn in isolation, without counter narratives from adults or whānau.

A broad range of research on porn usage among young people highlights how porn influences their sexual attitudes, beliefs and behaviours.

Porn also includes powerful learning elements, such as visual imagery, arousal, behavioural role-modelling, and physiological reinforcement, which can enhance its impact. Its integration into mainstream social media, digital platforms, and AI-driven sexual content has further amplified its reach and influence – and research has yet to fully explore how this intersection affects youth sexual beliefs and behaviours.

For young people growing up with online porn, viewing the normalisation of sexual violence can pose risks in shaping their attitudes and beliefs around sexual violence.

Studies conclude there is a significant relationship between viewing porn and the development of harmful sexual attitudes and beliefs towards women (Upton et al., 2020; Krahe et al., 2021; Lim et al., 2016; Peter and Valkenburg, 2009; Sun et al., 2016; Waterman et al., 2022), emphasising the following key themes:

- an increased likelihood of holding gender stereotypes, sexist attitudes, and endorsing the sexual objectification of women
- higher acceptance of sexual aggression and attitudes that support violence against women
- increased recreational attitudes towards sex and erroneous beliefs about sex
- increased rape-myth endorsement and victim blaming
- porn shaping males' sexual expectations through sexual scripting
- harmful gendered perceptions, such as perceived female enthusiasm for risky or rough sexual acts, and male adolescents perceiving porn as a realistic template and integrating these sexual scripts into real-life sex.

An article published in the British Journal of Criminology further highlights how the framing of sexual violence as normative in porn can attune, augment, and alter young people's attitudes and understandings of sexual violence (Vera-Gray et al., 2021).

Specifically, the portrayal of pleasure in response to sexual aggression and the absence of consent can contribute to problematic beliefs around consent, aggression, and distinguishing between pleasure and inflicting pain.

Locally, Māori academic Ahinata Kaitai-Mullane's (2022) analysis of depictions of wāhine Māori on Pornhub identified similar themes, noting that the fetishisation, control, domination, dehumanisation and objectification of wāhine Māori in porn can weave overwhelmingly harmful social narratives and carry the potential to create significant harm as they permeate society.

Studies centred around the relationship between porn viewership and the perpetration of risky and aggressive sexual behaviours conclude there is an influential relationship, underpinned by the way in which porn reflects and reinforces some of the drivers of sexual violence (Upton et al., 2020; Pathmendra et al., 2023; Lim et al., 2016; Mori, 2023; Donevan and Mattebo, 2017; Rodenhizer and Edwards, 2019; Wright et al., 2016; Waterman et al., 2022; Ybarra et al., 2018).

This relationship is also supported by media socialisation models, with evidence supporting the hypotheses of the Acquisition, Activation, Application model (3AM; Wright, 2011) regarding the role of sexual scripts in sexual media socialisation processes.

Key themes include:

- an increased likelihood of young people engaging in sexually dominant or risky sexual behaviours including earlier onset of sexual activity, unprotected sex, casual sex, choking/strangulation, name-calling, spanking, and casual sex
- a higher probability (4-10 times) of perpetrating four types of aggression: sexual harassment, sexual coercion, forced sex, and/or manipulative sex
- decreased bystander willingness and a reduced likelihood of intervening in acts of violence.

The strength of this relationship varies across studies, influenced by several potential mediating variables. For example, these behaviours are more prevalent among adolescents who frequently view violent pornography, use it as a primary source of sexual knowledge, or perceive its content as realistic. Conversely, adolescents who perceive pornography as less real experience a slower development of problematic sexual attitudes and behaviours over time.

The following sections outline key areas of risk and impact identified in the research.

3.4 INCREASED RISK OF FEMALE VICTIMISATION

Sexual violence victimisation is disproportionately experienced by female and sexually diverse young people. With the normalisation of sexual violence against women in porn, emerging research is exploring whether porn use may be predictive of sexual violence victimisation.

Preliminary studies suggest a potential relationship. For example, a recent US study found that female adolescents who viewed porn alongside engaging in online sex chats had a higher likelihood of intimate partner violence (IPV) and sexual assault victimisation (Maas et al., 2025).

Another study documented high rates of IPV victimisation among female adolescents who viewed porn, particularly among those with diverse sexual identities but porn was not a predictor (Herbitter, 2021).

Emerging data in Aotearoa on young women's experiences of rough sex and 'choking' indicate that the normalisation of these practices in porn and mainstream media has created social pressure to accept unwanted and aggressive sexual acts as a normative part of sex. This, in turn, can contribute to a broader risk of victimisation.

The relationship between engagement with online Dark Romance (see Section 2.4) and victimisation risk also warrants further exploration. For example, a recent study of female adolescent fanfiction writers found that those who expressed attraction to fanfiction 'bad boys' – characters depicted as sexually aggressive or manipulative – were more likely to report tolerating similar behaviours from real-life romantic partners (Hedrick, 2021).

3.5 ACCELERATED RISK OF HARMFUL SEXUAL BEHAVIOUR (HSB) IN VULNERABLE YOUTH

Exposure to porn can be a significant risk factor for HSB among young people with intersecting vulnerabilities such as sexual victimisation, impulsivity, neurodivergence, intellectual disability, poor social skills, or a disrupted care history.

For these young people, regular exposure to sexualised media featuring degradation and objectification can increase and accelerate the likelihood of engaging in HSB (Mori, 2023; Pathmendra, 2023).

Young people viewing CSAM face even greater risk due to the reinforced pairing of arousal with children – and the development of related fantasies (Sandvik, 2017). Some emerging research also suggests that porn may not only accelerate but actively contribute to HSB onset, with key amplifiers being exposure to sexualised environments, father figures validating porn use, the absence of an approachable adult, and access to violent porn and CSAM (Gerhard-Burnham, 2016; McKibbin, 2017; Sandvik, 2017).

While research on this relationship continues to evolve, it is important to recognise that vulnerable young people today face unprecedented risks, as their ease of exposure to harmful sexual content differs dramatically from that of earlier digital natives.

Cartoon, AI-generated, and mainstream content normalising HSB such as sex with minors, incest, and forced sex is now readily accessible across multiple platforms and can be difficult to avoid.

Insights from New Zealand’s HSB sector provide a critical perspective on these risks. Services have raised increasing concerns about the ease of access to ‘eroticised’ online sexual violence and its influence on adolescent clients’ perceptions of consent, coercion and violence – and what they consider safe, normal or expected. They describe porn as a core influence, which for young viewers can reinforce, normalise and affirm HSB.

Services also report growing concern over AI-generated objectionable content, with some clients arguing that, since it is “not real”, engaging with it causes no harm.

The role of porn and HSB among vulnerable young people is a critical area for research and intervention. While a direct causal link must be cautioned against, there is strong evidence of an influential and multi-faceted relationship.

3.6 SELF-GENERATED SEXUAL CONTENT AND AI COMPANIONS

Youth feedback from the 2022 The Light Project Creating Online Sexual Content resource project identified several risks for young people under 18 creating or selling self-generated sexual content.

These include consent breaches, content ownership issues, bullying, harassment, stalking, regret, secrecy, mental health issues, and exploitative situations when content is coercively generated or shared.

The project also highlighted that some young people are particularly vulnerable to being coerced into creating or selling content due to factors such as low income, poor social circumstances, low digital literacy, unhealthy relationships, or a lack of agency and information to make informed decisions.

These youth face a heightened risk of TFSV and exploitation. Interviews with young creators in Aotearoa, particularly those using platforms like OnlyFans, revealed parallels to the offline sex industry – but without the support, information, or safety measures typically available in that sector. Additionally, there is a lack of resources for

young people considering creating sexual content and insufficient support for those who experience harm. Young people under 18 noted that secrecy, social taboos, and shame surrounding sexual content often deterred them from seeking help when they experience harm.

Limited data exists on the rise of youth engagement with AI boyfriends and girlfriends, but feedback from The Light Project’s workforce training with schools, counsellors, and youth services highlights several risks.

AI companions are highly popular among teenagers, who are at a critical stage in their sexual, emotional, and social development. These companions are customised to cater 24/7 to the user’s desires, and lack the complexities, boundaries and consequences of human relationships. Many platforms also offer highly sexualised interactions intended for older audiences, which can be confusing for young people navigating real-world relationships.

This can lead to unrealistic expectations, reduced resilience in managing interpersonal conflict, and confusion around sexual safety, consent, and pleasure (SchoolTV, 2024).

Some young people also report emotional dependence or compulsive habits with AI companions, leading to secrecy, social isolation, and mental health challenges.

A recent AI Social companion risk assessment indicated AI companions can also encourage harmful behaviours and potentially exacerbate mental health conditions (Common Sense Media, 2025). The Australian eSafety Commissioner also highlighted a growing crisis, with schools reporting students spending up to 5 hours daily engaging, often sexually, with AI companions (Bharadwaj, 2024). In addition, many AI relationship platforms collect vast amounts of personal data, potentially exposing youth to safety issues, data breaches, or exploitation.

“We have recently witnessed a direct correlation between the significant downsizing of the trust and safety functions in many social media organisations and an increase in harmful online content.”

(Netsafe response to the Safer Online Services and Media Platforms Consultation, 2023)

3.7 INFLUENCE OF TV AND MAINSTREAM MEDIA

3.7.1 Media’s impact on sexual attitudes and behaviour

A meta-analysis found that media exposure consistently influences sexual attitudes, perceived peer norms, and behaviours.

The media portrays sex as common, recreational, and low-risk, shaping viewers’ sexual decision-making (Coyne et. al., 2019). The analysis revealed a stronger effect of sexualised media on behaviour than previously estimated, highlighting its substantial impact.

3.7.2 Reality TV and sexualised aggression

Greater reality TV consumption predicts stronger support for traditional heterosexual gender roles, which, in turn, is linked to greater acceptance of sexualised aggression over time.

The researchers found that participants who consumed more reality TV at the start of college tended to show greater support for traditional heterosexual gender roles one year later. Those who supported traditional heterosexual gender roles, in turn, tended to be more accepting of sexualized aggression

(Papp et al., 2022).

3.7.3 Sexting and media exposure

Among cisgender boys, sexually explicit reality TV and music videos are linked to active sexting behaviours, while pornography consumption is associated with sexting behaviours across all gender groups (Aubrey et al., 2024).

3.7.4 Rape myth endorsement and media

US college students who perceive media characters as similar to people they know are more likely to endorse rape myths that blame victims or exonerate perpetrators.

This association is stronger for men and does not rely on personal identification with media characters (Elmore et al., 2022).



4

The Aotearoa New Zealand Context

This section first surveys existing agencies within the family violence, sexual violence, health, charitable, and justice sectors.

It then offers feedback from national scoping projects with health and FVSV services across Aotearoa, highlighting workforce concerns, trends, and gaps related to the new digital sexual landscape. While there is some alignment with 'Te Aorerekura: National Strategy to Eliminate Family Violence and Sexual Violence', the current response is fragmented. A lack of government funding and coordinated investment has limited the ability to scale initiatives, sustain long-term efforts, support new research, or achieve national reach.

4.1 EXISTING AGENCIES

4.1.1 Te Mana Whakaatu – Classification Office

Te Mana Whakaatu – Classification Office (hereafter “Classification Office”) has played a pivotal role in addressing pornography and its impact on young people in Aotearoa New Zealand.

Its research has brought national attention to young people’s experiences with porn. In addition, it has developed a range of public resources for parents, and a resource module for schools and educators created in partnership with the Ministry of Education. The Classification Office also facilitated the cross-agency Pornography Working Group, which was formed in 2018 to promote collaboration and awareness of youth and porn-related issues. In 2024, this group formally closed and was replaced by an information-sharing annual hui open to a wider group of stakeholders.

4.1.2 The Light Project

The Light Project is a workforce development service specialising in the new digital sexual landscape.

It equips and strengthens the workforce with primary prevention, early intervention, and response training and resources to support young people in navigating their digital sexual world safely.

The Light Project’s two websites, Light Project and In the Know, are New Zealand’s leading go-to platforms for information, tools and support on the digital sexual landscape for youth, families, and youth services. The Light Project has collaborated with ACC, the Ministry of Social Development (MSD), and Health New Zealand – Te Whatu Ora on workforce development training, scoping and resource development projects for national family violence/sexual violence (FVSV) services, youth, and health services. The Light Project supports a kaupapa Māori response to rangatahi Māori and the digital sexual landscape, maintaining strong strategic relationships with Te Rau Ora, national Māori health workforce development organisation.

4.1.3 Te Whatu Ora Workforce Development Programme

Te Whatu Ora is currently implementing a widespread national health workforce development programme entitled The Online Sexual Landscape and Young People in Aotearoa: Developing a Skilled Health Workforce, which aims to reduce the risk of online-related sexual violence for children and young people.

The programme is focused on building a skilled, confident and capable health workforce through national sector training; the development of a workforce Youth and Porn Toolkit; and the integration of the digital sexual landscape into health policy and practice. The programme also fulfils key Te Whatu Ora responsibilities under Te Aorerekura, specifically Shifts 3, 4 and 6.

4.1.4 Ministry of Social Development youth and porn initiatives

MSD has commissioned several innovative resources to address young people's concerns about porn and the digital sexual landscape.

These include the In The Know youth website and the 16-part In The Know video series, which offer youth-friendly and safe tools, tips and information on porn. In response to emerging trends, MSD commissioned The Light Project's "Curious about Rough Sex and Choking?" and "Considering Creating Sexual Content?" alongside "Check It Out" – resources for young people concerned about their online fantasies and behaviours. Their current ground-breaking campaign, "Love Creep", directly engages with the digital space by highlighting how online stalking, coercion and device control can be used to facilitate sexual harm. Additionally, in 2024 MSD funded the Youth and Porn: FVSV Workforce Development and Scoping Project to better understand and strengthen sector capacity in the digital sexual space.

4.1.5 Oranga Tamariki

Oranga Tamariki recently commissioned the development of "Press Pause", an interactive online hub designed to support school staff, counsellors, and youth agencies in managing and preventing concerning and harmful sexual behaviours.

The site features modules on concerning online behaviour and pornography, providing information on how to understand, recognise, and respond to issues in these areas.

4.1.6 ACC

In 2021, ACC commissioned the Youth and Porn: FVSV Workforce Development and Scoping Project, which included the delivery of 82 training workshops for facilitators of Mates & Dates education programme and sensitive claims counsellors, alongside an FVSV scoping report.

4.1.7 Academic research

A broad range of research is currently underway among academics across Aotearoa exploring the impact of the digital sexual landscape on youth sexual culture.

This includes seminal work on pornography, rough sex, and 'choking' / sexual strangulation by Samantha Keene and Nicola Gavey. Nicola's research has also explored image-based sexual abuse, as has Claire Meehan's work on nudes, sexts and porn among young people. Led by Nicola Gavey, Octavia Calder-Dawe, Kris Taylor and others, Shifting the Line is a current project focused on building critical thinking around gender, sexism and online ethics. Jade Le Grice, Jan Jordan and Siobhan Healey-Cullan have also contributed to a deeper understanding of pornography and sexual violence, and porn literacy pedagogies. This research provides valuable insights into emerging online sexual norms, and as experts in this evolving space, academics should play a vital role in any national responses to youth and the digital sexual landscape in Aotearoa.

4.1.8 Makes Sense

Makes Sense is a New Zealand organisation committed to tackling online sexual harm by addressing the root causes through systemic and policy-level changes.

Its mission is to create safer online environments for all children and young people by advocating for stronger protections at both government and industry levels. Make Sense's achievements include a significant reduction in rape content on a prominent search platform, the adoption of the Internet Watch Foundation (IWF) filter which increased CSAM filtering to up to 30,000 URLs daily, and ongoing improvement of internet filtering of primary school devices.

4.1.9 Safe Surfer

Safe Surfer is an innovative platform that protects kids from harmful content like graphic violence, malware, illegal sites and pornography.

The Samsung x Safe Surfer Kid-Safe Smartphone provides parents with choice over what and how much their children can access via their smartphone or tablet devices. Three levels of functionality range from access to calls, texts and camera only to allowing safe internet browsing and monitored internet access as kids mature. Safe Surfer has long been an advocate for online safety in New Zealand to keep children safe online.

4.1.10 Netsafe

Netsafe helps children to navigate concerns related to their digital safety, such as grooming, bullying, illegal content and scams.

Parents and youth can contact Netsafe seeking support. Upon requests for further information or evidence, Netsafe staff provide direct advice, including options for taking content down, mediation or negotiation with the other parties, and/or referrals to other agencies. Netsafe has a Youth Action Squad promoting safer, more positive online experiences and responsible citizenship nationwide. Netsafe is the approved agency under the Harmful Digital Communications Act 2015 (HDCA) to handle complaints, offer mediation, and make referrals to the Ministry of Justice for criminal offences. Netsafe implements national programmes such as Sticks 'n Stones and campaigns like Spicy Noods.

4.11 Department of Internal Affairs (DIA) Digital Safety Group and campaigns

DIA, through its Digital Safety Group, leads New Zealand's response to online child sexual exploitation material (CSEM).

Its work here spans CSEM detection, prevention and enforcement under the Films, Videos, and Publications Classification Act 1993. DIA work with Customs and New Zealand Police under the banner of "Taskforce Ruru" for victim identification investigations. They collaborate internationally with agencies like INTERPOL and International Association of Internet Hotlines (INHOPE). DIA operates the DCEFS, which includes the IWF blocklist. The department promotes public awareness through campaigns such as "Keep It Real Online", which provides tailored resources for children, teens and parents. The department also hosts the Combatting Child Exploitation Online Hui quarterly.

4.1.12 Wider community-led initiatives

Several small, community-led initiatives are helping young people build online resilience and prevent digital sexual harm.

Digital Waitaha Charitable Trust in Ashburton supports youth through education, digital equity advocacy, research, and whānau workshops. In Te Tai Tokerau, the Taihono initiative, led by Tuhiata Mahiora, focuses on reducing online harm by helping rangatahi disconnect from harmful digital environments and foster real-world connection. Taranaki Safe Families Network are currently implementing a comprehensive community-led cross-agency workforce development and community mobilisation response to the digital landscape across Taranaki.

Though currently limited in scale, these efforts show the value of community-driven approaches in supporting a wider national response to online safety.

4.2 YOUTH AND FVSV SECTOR FEEDBACK: TRENDS AND HARMS

Several national scoping projects have been conducted with health and FVSV services across Aotearoa to assess workforce concerns, trends and gaps related to the new digital sexual landscape.

Across these projects, ninety-eight per cent of services identified porn and the digital sexual landscape as highly relevant issues (The Light Project, Scoping Project Report for MSD FVSV Sectors, July 2024 and ACC Workforce Development Project Scoping and Findings Report, January 2022). Services highlighted key trends they believe are influenced by widespread access to porn, shifts in sexual norms shaped by online content, and increased youth engagement in online sexual activities. With research struggling to keep pace with the rapidly evolving digital landscape and limited research scope in Aotearoa, this frontline feedback provides critical insights into emerging trends and challenges affecting young people. Key themes are outlined below.

4.2.1 New youth sexual norms

Porn and online sexual content increasingly serve as primary sources of sex education for youth, influencing sexual attitudes, expectations and behaviours.

Observed trends include the normalisation of diverse sexual behaviours, an acceptance of sexual aggression as part of sex, attitudes that support sexism, and rigid gender roles and stereotypes.

4.2.2 Normalisation of rough sex and 'choking' / sexual strangulation

The growing acceptance and normalisation of rough sex and 'choking' within youth culture has been described as a critical FVSV concern.

Services describe these practices as "accepted and expected" and are seeing an escalation of cases presenting in workplaces, with adult sexual assault assessment and treatment services seeing choking among admissions rising from 2 to 25% in recent years.

International research corroborates this trend, showing high prevalence rates among young people (40-70%), which raises significant health risks, including long-term neuropsychological damage and the risk of death from choking (Herbenick, 2021).

4.2.3 Technology-facilitated sexual violence and image-based harms

There has been a significant rise in TFSV and image-based sexual harms recently, including revenge porn, grooming, coercive image creation, unsolicited nudes, AI-generated deepfakes, online sexual bullying, sexual assault in virtual environments (avatar-to-avatar), and predatory online behaviour.

TFSV can profoundly impact youth mental health, often resulting in shame, anxiety, isolation, depression, paranoia, fear and regret.

These emerging forms of image-based harm pose unique challenges for a workforce primarily experienced with 'offline' sexual harm. The generational digital gap has made it difficult for some services to provide effective support for cases of abuse influenced by, or occurring in, the digital realm.

4.2.4 Mental health issues

The impact of online sexual engagement on young people’s mental wellbeing is a rapidly mounting concern.

Services have observed a rise in youth struggling with managing their online usage, shame, compulsive and secret sexual online behaviour, evolving porn use, problematic relationships with AI sexual companions, intrusive thoughts, withdrawal, and adverse effects on relationships and daily functioning.

4.2.5 Increased sexual harm and blurred views on consent

There has been a rise in online sexual harms that services believe are related to the normalisation of diverse sexual behaviours online.

These include harmful rough sex, unwanted anal sex, rapid penetration, forced sex, ‘consensual-non-consent’ acts, and a rise in sibling or child-to-child sexual assault. Additionally, youth understandings of consent are increasingly blurred, with some young people not recognising harmful experiences as assault, due to the normalisation of these behaviours online.

4.2.6 Impacts on sexual relationships

Online sexual content is shaping some young people’s sexual expectations affecting partner, peer, and familial relationships.

Services have observed increasing youth pressure to watch and perform diverse sexual acts seen online, share sexual images, agree to sexual acts being filmed, and meet unrealistic sexual expectations from partners.

4.2.7 Porn reinforcing violence and HSB

The sexual harm workforce reports that the rise in access to mainstream sexual content that normalises violent and illegal sexual acts (such as forced sex, bestiality, and family sex) poses growing risks for their clients.

This content can reinforce problematic sexual norms and harmful sexual behaviours, especially among clients with pre-existing vulnerabilities. These services also reported an increase in their clients using online platforms for perpetrating HSB.

4.2.8 Risks for vulnerable youth

The new sexual landscape presents heightened risks for vulnerable youth.

Services report that these young people are more likely to experience early or accidental exposure to illegal content, adults exposing them to pornography, triggering of past trauma, online grooming, problematic porn use (PPU), and coercion to create or sell sexual content. They also highlighted that early exposure to porn may increase the likelihood of vulnerable youth developing attitudes and behaviours supportive of violence.

4.2.9 AI platforms

There has been a significant rise in young people, particularly school students, engaging with AI-generated sexual platforms including AI porn sites, AI undress or ‘nudify’ apps, and AI companions.

Services report notable risks and harms related to these platforms, including the non-consensual creation and sharing of AI deepfakes and problematic relationships with AI companions, which can lead to secrecy, social isolation, mental health issues, and challenges in navigating real-world relationships.

4.3 YOUTH AND FVSV FEEDBACK:
SKILLS AND CAPABILITIES

FVSV and youth health services in Aotearoa report crucial gaps in workforce knowledge, skills, and capability regarding the digital sexual landscape affecting children and young people.

The recent MSD report outlining FVSV services gaps in Aotearoa identified a lack of understanding of online sexual harm and pornography as a critical national gap (MSD, 2024).

Recent national FVSV workforce surveys indicate only 13% of professionals rate their knowledge as 'good,' while 82% report their service lacks knowledge, skills and resources (The Light Project, Scoping Project Report for MSD FVSV Services, July 2024).

Services highlight that the rapid changes in the digital landscape, generational gaps, and a lack of training and resources to guide practice, prevention or response initiatives have left them ill-equipped to prevent harm or support young people in safely navigating their digital sexual environments.

Key identified gaps in knowledge and skills include:

- understanding the digital sexual landscape trends, platforms, and emerging technology
- impacts of online sexual content on sexual wellbeing, development, relationships, and new sexual norms around sexual violence
- risks and harms including TFSV, IBA, and harms contributed to by online norms
- primary prevention strategies to integrate critical thinking and online resilience into existing violence prevention models and initiatives
- assessment tools for TFSV; IBA; online-related harms such as forced sex, rough sex, and 'choking' / sexual strangulation; and PPU
- brief intervention strategies for frontline services on TFSV, IBA, PPU, harmful online-related sexual fantasies and behaviours, exposure to CSAM, and rough sex, and 'choking' experiences
- response pathways and management for TFSV, IBA, PPU, rough sex, and 'choking'
- tools and resources to support families and communities.

Services recommend sector-wide training, resources and support to address these gaps.



5

Aotearoa New Zealand Regulatory and Policy Approaches

An examination of New Zealand's approach in contrast to international models, including Australia, the United Kingdom, Canada, and the European Union, reveals best practices and regulatory innovations that could inform more robust and coordinated protections for children in Aotearoa.

5.1 AOTEAROA NEW ZEALAND

To address online sexual harm, Aotearoa focuses on CSAM and child sexual exploitation and abuse (CSEA), but its strategic and legislative framework fails to address other portrayals of online illegal sexual content (e.g. rape, bestiality) nor does it hold tech platforms accountable for their role in hosting such material.

New Zealand’s current online regulatory system shows signs of fragmentation and limited capacity, making it difficult to respond effectively to emerging online risks. (Daubs, et al, 2021; Frykberg, 2024; RNZ, 2024; Whyte, 2024). There are no age-assurance requirements for adult websites or social media.

NATIONAL STRATEGIES AND ACTION PLANS FOCUSED ON CHILD SAFETY ONLINE

Te Aorerekura: National Strategy to Eliminate Family Violence and Sexual Violence is a 25-year strategy launched in December 2021 and overseen by Te Puna Aonui, an interdepartmental executive board created under the Public Service Act 2020. The broad focus is on addressing physical, in-person harm, particularly within the family context. Sexual abuse online is mentioned on page 10 of the National Strategy, within a definition of sexual violence. However, there are no dedicated actions addressing primary prevention around harmful online sexual norms and building critical thinking on pornography, online sexual abuse prevention, digital platform accountability, or child online safety initiatives and frameworks to build resiliency or foster protective factors - a critical gap considering the scope and severity of harm children and young people face online. There are also no dedicated actions around building workforce skills and capabilities around the digital sexual landscape, or the development of prevention, early intervention and response resources. While Te Aorerekura has signalled an update to its Action Plan by the end of 2025 to include themes such as “preventing violence before it starts” and “taking action on sexual violence”. It is important to note that online sexual violence, or increased likelihood of violence because of online sexual experiences, is not yet addressed in the plan implementation.

The **Child Youth and Wellbeing Strategy (CYWS)** aims to address child welfare. In the 2024-2027 iteration of the National Strategy, there is no mention of online or digital safety. CYWS is aligned with Te Aorerekura.

The **Plan of Action Against Forced Labour, People Trafficking and Slavery 2020–2025** has a cross-agency approach. “Government will consider next steps for the Plan beyond 2025 in due course, recognising that children are among the most vulnerable to exploitation both within New Zealand and internationally.” (Ministry of Business, 2025)

5.1.1 Legislative/statutory framework

New Zealand lacks dedicated legislation focused on addressing online harm. Instead, there is a reliance on three key laws which focus on objectionable content, CSAM, and post-harm enforcement:

- **Films, Videos, and Publications Classification Act (FVPCA) 1993:** Governs the classification of publications including films, commercial video-on-demand (CVoD), and games. Key amendments: In 2005 its jurisdiction was extended to internet-based objectionable material, increasing penalties; in 2020 CVoD content regulation was incorporated.
- **Harmful Digital Communications Act 2015:** Governs responses to digital harm: online bullying, harassment, revenge porn, and digital abuse.
- New Zealand combats CSAM at the border under the **Customs and Excise Act 2018**, using intelligence-led screening and targeted interventions to detect and intercept offenders importing CSAM.

Draft Members’ Bills include: Social Media Age-Restricted Users Members Bill (Catherine Wedd, May 2025), and Deepfake Digital Harm and Exploitation Members Bill (Laura McClure, May 2025).

5.1.2 Enforcement mechanisms

Harmful Digital Communications Act 2015: Netsafe is the approved agency to handle complaints, offer mediation, and make referrals to the Ministry of Justice for criminal offences. The HDCA currently lacks the agility to tackle emerging threats such as sextortion and AI-generated deepfake abuse because “intent to cause harm” must be proven (Higgins, 2024; Hunt, 2024).
The Aotearoa New Zealand Code of Practice for Online Safety and Harms was launched in 2022 by Netsafe and NZTech, involving Meta, Google, TikTok, Twitch and X. It is a voluntary, self-regulatory framework with no enforcement powers.
The role of Te Mana Whakaatu – Classification Office is to classify films, videos and publications under the FVPCA 1993. Any content that promotes or supports the sexual exploitation of children or young people is illegal.
DIA enforces the FVPCA 1993 in regard to CSAM offences through a cross-agency approach with New Zealand Police and Customs (Taskforce Ruru). Digital Safety Inspectors within DIA hold specific warrants under the Search and Surveillance Act 2012 to investigate CSAM. Other illegal sexual content is not addressed, however. Government funding cuts in 2024 has likely impacted DIA’s capacity.
The Digital Child Exploitation Filtering System, managed by DIA, operates a block list for CSAM, including the Internet Watch Foundation (IWF)’s CSAM block list. There are issues with HTTPS. This is not mandated for ISPs to use, but three major internet service providers do employ this system.
The New Zealand Customs Service targets the cross-border movement of CSAM, both physical and digital. Customs’ Child Exploitation Operations Team experienced notable staffing cuts in 2022, despite rates of child exploitation increasing.

International partnerships: Online Child Exploitation Across New Zealand (OCEANZ), is a specialist team within New Zealand Police that is part of a Virtual Global Taskforce. It collaborates with the US National Center for Missing and Exploited Children (NCMEC), the International Association of Internet Hotlines (INHOPE), INTERPOL and WeProtect Global Alliance. Member of Five Eyes and the Voluntary Principles to Counter Online Child Sexual and Abuse.

5.1.3 Previous attempts at regulation

The Safer Online Services and Media Platforms (SOSMP) review: Launched in 2021 by DIA with support from the Ministry for Culture and Heritage, the SOSMP review aimed to modernise New Zealand's outdated content regulation system (which is reliant on the FVPCA) with a focus on reducing online harm.

Despite strong support from stakeholders and industry, the 6th National Government scrapped the initiative after being elected in 2023, citing concerns over free speech and regulatory overreach. This move coincided with funding and staffing cuts to DIA, undermining efforts to tackle online child exploitation (DIA, 2023; Donnell et al., 2024; Goatley et al., 2023; Van Velden, 2024).

Although not intended as a step toward broader regulation, the Pornography Working Party (PWP) represented a significant initiative. While porn is legal for those 18 years and older in New Zealand, there is no online age verification (AV) system to enforce this. In its final 2022 Cabinet briefing, the PWP recommended AV technology be included within the SOSMP review. However, with little government action, the PWP was disbanded and replaced by an annual information-sharing hui, with efforts now focused on education.

“Online porn is easily accessible for young people and even children in New Zealand – on their smartphones and other devices. Right now, there is no comprehensive mechanism in place to prevent access in New Zealand.”

(Classifications Office, Submission on the Safer Online Services and Media Platforms, July 2023)

5.2 INTERNATIONAL REGULATORY OVERVIEW

A high-level summary of the regulation approaches taken by **Australia**, the **United Kingdom**, the **European Union**, **USA** and **Canada** is provided below.

Online Safety Legislation	Australia	UK	EU	USA	Canada	NZ
Online Safety Law	Online Safety Act 2021	Online Safety Act 2023	Digital Services Act	IP -Draft KOSPA/ COPPA 2.0	In Progress - Draft Bill C-63	Nil
Safety by Design approach	Y	Partially	Y	In Progress	In Progress	N
Secure by Design approach	-	Y	Y	IP	IP	N
Narrow coverage/ Content focussed (narrow focus on illegal content like CSAM, content that is harmful to children)	Y	Y	Y	IP	IP	N
Broad coverage/ Systems focussed (safety by design, child safety, design principles, privacy)	-	Y	Y	IP	IP	N
Duty of care approach	Y	Y	-	IP	IP	N
Risk Mitigation approach	Y	Y	Y	IP	IP	N
Detailed definition of illegal content and different approaches of law to different types	Y	Y	-	IP	IP	N
Flexible definition of illegal content and law applies to all types of illegal content	-	-	Y	IP	IP	N
Generative AI legal capabilities	Y	Y	Y - AI Act	IP	IP	N
Algorithm/dark pattern restrictions	IP	Y	Y	IP	IP	N
Bans on targeted advertising profiling children	IP	Partially	Y	IP	IP	N
Transparency Reports						
Strong transparency and reporting requirements with prescribed metrics. Includes detailed risk assessments.	Y	Y	Y	IP	IP	N
Risk Assessment required	Y- Due 21 June 2025	Y- Due July 2025	Y - Due 16 March 2025	IP	IP	N
Voluntary reporting	N	N	N	IP	IP	Y
Independent Regulator						
Independent Regulator or competent authority: - enforcement power - Information gathering power	Y - eSafety	Y - Ofcom	Y - Digital Services Coordinator/ CCommission	IP	IP	N
The Industry drafts standards or Codes	Y	N	Y	IP	IP	N
Regulator "holds the pen" / defines the standards or codes	N	Y	N	IP	IP	N
Strong powers to enforce compliance/redress - strong penalties /fines for non-compliance	Y 30,000 penalty units (currently AUD \$9.9m)	Y up to £18 million or 10% GAT	Y up to 6% GAT	IP	IP	N
Turn off powers- for failures to comply	N	Y	Y	IP	IP	N
Strong public facing complaints system	Y	Y	Y	IP	IP	N

5.2.1 Australia

Australia uses a comprehensive framework to protect children online combining strategy, policy, law, enforcement, education and industry collaboration. The government supports a whole-of-government, multi-agency response and proactive industry action.

NATIONAL STRATEGIES

The **National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030** outlines a coordinated, long-term approach to tackling child exploitation online and offline. The National Office for Child Safety oversees the National Strategy and works closely with the National Centre for the Prevention of Child Sexual Abuse, which is to receive \$22.5 million over 5 years (from 2021).

The National Strategy aligns with the **Safe and Supported: The National Framework for Protecting Australia’s Children 2021-2031**.

The **Aboriginal and Torres Strait Islander Action Plan 2023-2025** aligns with the National Strategy to ensure culturally competent, trauma-informed policies and services.

LEGISLATION

Online Safety Act 2021: Requires online service providers to take steps to protect children from harmful material, regulate violent content (including rape), assess and mitigate risks, limit the availability of child exploitation content, and comply with industry codes and standards for dealing with illegal and harmful content.

- The 2024 **Basic Online Safety Expectations (BOSE)** framework requires digital platforms to take proactive measures against CSAM, cyber abuse, and exploitative content.
- **Age verification for pornography websites:** eSafety commenced an “Age Assurance Technology Trial” in May 2024, encompassing both age verification and age estimation technologies, to explore the efficacy in protecting children from encountering pornography and other high-impact online content”. The final report on a trial exploring different age-assurance technologies is due in June 2025 (eSafety, 2024).

Criminal Code Amendment (Deepfake Sexual Material) Act 2024: Specifically governs the use and abuse of deepfakes.

Online Safety Amendment (Social Media Minimum Age) Act 2024: Sets a mandatory minimum age of 16 for major social media platforms, with age assurance required. The Age Assurance Technology Trial will inform action taken.

The Online Dating Industry Code (October 2024) requires online dating platforms to implement systems to detect and address potential incidents of online harm.

Online Safety Amendment (Digital Duty of Care) Bill 2024: Mandates continuous risk assessment and mitigation by platforms to prevent bullying, predatory behaviour, and algorithm-driven harmful content. Lapsed at dissolution 28 March 2025.

“eSafety uses its world-leading regulatory powers to implement and enforce Australia’s online safety laws.”

(eSafety, 2024)

Enforcement mechanisms: The eSafety Commission, an independent regulatory authority, leads online safety nationwide. eSafety can enforce content takedown notices, impose penalties, and oversee compliance with safety expectations. A new technologies risk-assessment tool assesses risks before the launch of a platform. It is led by the eSafety Commissioner. The **Australia Federal Police (AFP)** investigate child exploitation. In 2023, AFP and Monash University developed an AI model to detect CSAM on the dark web. **The Australian Centre to Combat Child Exploitation (ACCCE)** was established in 2018 by AFP. This has become a key enforcement agency, facilitating national collaboration.

International partnerships: The ACCCE facilitates international collaboration to combat child exploitation, working alongside the National Office for Child Safety and law enforcement agencies, as well as the NCMEC. Member of Five Eyes and the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse.

5.2.2 United Kingdom

The United Kingdom employs a similar model to Australia, with strategy, and a statutory regulatory framework to protect children online, led by Ofcom under the Online Safety Act 2023.

The UK model imposes legally binding duties of care on platforms, with Ofcom as the independent regulator empowered to enforce compliance.

“To tackle child sexual abuse in all its forms, we need everyone to play their part. That is why I am delivering a national strategy to drive action across every part of Government, across all agencies, all sectors, charities, communities, technology companies and society more widely.”

(Priti Patel, UK Home Secretary, 2021)

NATIONAL STRATEGIES

The **Tackling Child Sexual Abuse Strategy 2021** is focused on preventing, tackling and responding to child sexual abuse in all its forms.

The **UK Council for Internet Safety** is a collaborative body including government departments, law enforcement, academia, industry and charities to ensure child internet safety.

The **Ending Violence Against Women and Girls Strategy 2024–2031** (EVAWG) is a whole of society approach that addresses GBV, abuse and harm including online and TCA, including cyberstalking, cyber flashing, sexual harassment, grooming for exploitation or abuse, image based sexual abuse and abuse through emerging technologies such as ‘internet of things’ devices.

The **Domestic and Sexual Abuse Strategy 2024–2031** is closely aligned with EVAWG.

LEGISLATION

The **Online Safety Act (OSA) 2023** introduces a legal framework requiring platforms to take greater responsibility for user safety. Providers must reduce risk, swiftly remove illegal content, and prevent children from accessing harmful or age-inappropriate material. The Act imposes a statutory duty of care, requiring companies to design safer systems across all user-facing services, including search engines and adult sites. It mandates proactive detection and removal of CSAM, with significant financial penalties for non-compliance (Clarkson et al., 2024; Fry, 2024; WeProtect Global Alliance, 2024).

The **Independent Pornography Review** has been led by Baroness Gabby Bertin since December 2023. Its recommendations were made in February 2025.

The **Children’s Code (September 2020)** focuses on the protection of children’s personal data, and is enforced by The Information Commissioner’s Office (ICO)

The **Crime and Policing Bill 2025** introduces a new offence that criminalises AI models that have been optimised to create CSAM.

Enforcement mechanisms: Under the United Kingdom’s OSA, Ofcom is the sole statutory regulator, responsible for setting codes of practice, establishing transparency requirements, conducting investigations, and issuing fines for non-compliance. Several other agencies play supporting roles in the broader online safety landscape. The **Child Exploitation and Online Protection Command**, part of the **National Crime Agency**, focuses on tackling online child exploitation. The **UK Council for Internet Safety** acts as an advisory body. The **Tackling Organised Exploitation Programme** and the newly formed **Child Sexual Exploitation Police Taskforce** (2024) support law enforcement responses to online harms, particularly organised or large-scale abuse.

International partnerships: The UK Government collaborates with the Global Partnership for Action on Gender-based Online Harassment and Abuse (Global Partnership), IWF, NCMEC and Stop It Now! (helpline and online support for people concerned about their own sexual thoughts, feelings or actions towards children). Member of Five Eyes and the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse.

“The Internet has been an amazing force for good, but it has caused undeniable suffering and can be an especially harmful place for children and vulnerable people. Behaviour that is unacceptable in real life is unacceptable on a computer screen.”

(Karen Bradley, UK Secretary of State for Digital, Culture, Media and Sport, 2017)

5.2.3 Canada

NATIONAL STRATEGIES

The National Strategy for the Protection of Children from Sexual Exploitation on the Internet 2004 is led by Public Safety Canada in partnership with the Royal Canadian Mounted Police, Justice Canada and the Canadian Centre for Child Protection (C3P). The National Strategy outlines a comprehensive, coordinated approach to “enhancing the protection of children on the Internet and pursuing those who use technology to prey on them” (Public Safety Canada, 2022).

The National Action Plan to End Gender-based Violence 2024 builds on federal initiatives and existing programmes (Government of Canada, 2024).

LEGISLATION

Proposed Online Harms Act (Bill C-63): This Bill has a “duty of care” focus and aims to hold platforms accountable for harmful content, including child exploitation. Bill C-63 has passed its second reading and is currently being reviewed by a parliamentary committee.

Proposed (Bill S-210) The Protecting Young Persons from Exposure to Pornography Bill is currently before the Canadian Senate. This Bill will criminalise making sexually explicit material available to a young person on the internet.

“Online child pornography incidents accounted for 87% of all police-reported online child sexual exploitation incidents in 2023.”

(Public Safety Canada, 2025)

Enforcement mechanisms: The Royal Canadian Mounted Police National Child Exploitation Crime Centre (NCECC) is the lead enforcement body under Canada’s National Strategy, coordinating national investigations into CSAM. A supporting role is played by the Department of Justice, which provides legal advice, training and policy support. C3P operates Cybertip.ca (Canada’s tipline for reporting online child sexual exploitation) and Project Arachnid, which detects and helps remove CSAM. Provincial and municipal Internet Child Exploitation Units handle local investigations and collaborate with the NCECC.

International partnerships: The Canadian Government collaborates with the NCMEC, G7 Child Sexual Exploitation and Abuse Working Group, WeProtect Global Alliance, and the Virtual Global Taskforce. Member of Five Eyes and the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse.

5.2.4 EUROPEAN UNION

The European Union (EU)’s approach to online safety for children is based on strong legal protections, platform accountability, and child rights by design. It combines legislation, guidance and cooperation between governments, industry and civil society.

STRATEGIES

- EU Strategy for a More Effective Fight Against Child Sexual Abuse 2020–2025
- Combatting Child Sexual Abuse Directive
- The European Strategy for a Better Internet for Kids (BIK+) (May 2022)

LEGISLATION

Digital Services Act (DSA) 2022: This Act sets unified rules for digital platforms across the EU, particularly against illegal content and CSAM with a duty of care focus. It offers stronger child safeguards than the United Kingdom’s OSA. Key requirements include measures to protect children’s safety, privacy and rights, age verification, and transparency reports on content moderation and risk management (OECD, 2024).

The DSA is supported by the EU General Data Protection Regulation, which sets the digital age of consent at 16 in most EU countries and is complemented by voluntary initiatives like the **EU Code of Conduct on Hate Speech** and the **Alliance to Better Protect Minors Online**.

Enforcement mechanism: The DSA is carried out by national Digital Services Coordinators, with the European Commission overseeing compliance for very large online platforms (VLOPs) and very large online search engines (VLOSEs).

5.2.5 ADDITIONAL COUNTRIES TAKING NOTABLE STEPS

FRANCE

The **Law on Securing and Regulating the Digital Space (the SREN Law)** was adopted in April 2024. It introduced a mandatory age verification system to block minors from accessing online pornography, granting Arcom – the French broadcasting authority – extensive new enforcement powers both domestically and internationally. France’s 2023 **Digital Majority Law | Loi sur la majorité numérique** requires social media platforms to verify users’ ages, get parental consent for those under 15, allow parents to suspend accounts, and include screen time limits for children.

IRELAND

Online Safety and Media Regulation Act 2023: This Act establishes a framework for regulating online safety in Ireland, including the formation of the Coimisiún na Meán, Ireland’s independent, and primary, media regulator.

UNITED STATES

Kids Online Safety and Privacy Act (KOSPA): This proposed legislation was first introduced to Congress in 2022, aiming to better protect children and teens online. Though not yet enacted, the 119th Congress is expected to revive it, with a stronger focus on CSAM and limiting Big Tech’s Section 230 immunity.

The Utah State Legislature passed **House Bill 465 and Senate Bill 194** during the 2024 General Session to protect minors who are on social media platforms. These Bills, collectively known as the Utah Social Media Act, have been temporarily suspended due to legal challenges.

The **App Store Accountability Act (SB 142)** passed out of the Utah Senate and will head to Congress in 2025.

Florida’s FL SB 1680 covers CSAM and computer generated CSAM. This may be generated CSAM of real children.

Louisiana’s LA SB 175 covers computer generated (AI) CSAM.

California’s AB 602 covers non-consensual deepfakes.

Tennessee’s TN HB 2163 covers computer generated CSAM. Additionally, the Ensuring Likeness, Voice and Image Security (ELVIS) Act.

Mississippi’s MS HB 1126 covers computer generated CSAM. It also passed Senate Bill 2577 which creates criminal penalties for using the creation of images or audio through AI which is published with the intention to cause violence, harm or deter someone from voting.



6

Technology and Industry

This section begins by canvassing the international organisations, tech platforms and governments worldwide that have developed methods to detect, block and remove online sexual abuse material and formed collaborations to reduce the risk of online harms.

Other key ways used to protect children online include built-in parental controls, family filters and age assurance. Considerations at the design and conception phase by tech companies can address potential future harm. This section also outlines 'Safety by Design', a concept that puts the onus on platforms to meet bare minimum requirements to keep young people safe.

6.1 TECHNOLOGY INITIATIVES THAT ADDRESS SEXUAL ABUSE AND INTERACTIONS

A number of international organisations are at the forefront of the detection, blocking and removal of currently known, new and novel child sexual abuse material (CSAM).

6.1.1 Internet Watch Foundation (IWF)

The IWF is a charity based in the United Kingdom focused specifically on the detection and creation of CSAM block lists, hashes (digital fingerprints) and machine models. The UK Government has provided IWF with a connection to its Child Abuse Image Database so that IWF can share hashes with the industry to allow more CSAM to be identified and removed. (iwf.org.uk)

6.1.2 Canadian Centre for Child Protection (C3P)

C3P manages Project Arachnid, an automated web crawler that detects and processes tens of thousands of images per second and sends takedown notices to online service providers to remove CSAM globally. (projectarachnid.ca)

6.1.3 StopNCII.org (Stop Non-Consensual Intimate Image Abuse)

StopNCII.org is a free global tool to protect non-consensual intimate images from being shared online by perpetrators of image-based abuse. StopNCII.org creates hash of an intimate image so it can be blocked from sharing on participating platforms. (stopncii.org)

6.1.4 Artificial Intelligence for Law Enforcement and Community Safety (AiLECS) Labs

The AiLECS labs are a joint initiative between Monash University and the Australian Federal Police, with a focus on leveraging AI to detect CSAM and develop technological interventions. Their research includes detecting deepfakes and image poisoning, which are increasingly relevant in the context of online sexual exploitation. (ailecs.org)

Emerging forensic technology tools are being developed to detect AI-generated CSAM and deepfakes. These advancements are crucial because the sophistication of online exploitation tactics is constantly evolving, necessitating equally advanced detection methods.

The global tech industry has formed alliances to try to collectively reduce some of the biggest online safety harms: online grooming, sextortion, CSAM, and intimate imagery.

6.1.5 ROOST (Robust Open Online Safety Tools)

ROOST provides free, open-source AI tools to improve the identification and removal of CSAM. The Christchurch Call announced a partnership with ROOST consortium to intensify efforts to eliminate terrorist and violent extremist content online. ROOST was launched in 2025 by a consortium of tech companies, including Google, OpenAI and Discord. (roost.tools)

6.1.6 Project Lantern

Project Lantern shares user data 'signals' of high risk of offending between the tech companies in a privacy-preserving way to prevent future harm and victimisation. It was launched by the Tech Coalition in 2023 with partners including Discord, Google, Meta and Roblox.

6.2 OVERVIEW OF BUILT-IN PARENTAL CONTROLS

Apple, Google and Microsoft all offer built-in parental control systems for their ecosystems, respectively called Screen Time, Family Link, and Family Safety.

While a range of third-party tools are also available, many parents report being overwhelmed by the number of options and the inconsistent quality of these solutions.

All three companies comply with the US Children's Online Privacy Protection Act (COPPA) of 1998, which mandates parental control enforcement only up to age 13. After this age, children are given the option to disable such controls. Apple's parental controls have received criticism, particularly around the persistent loopholes and reliability issues that often emerge after iOS updates. Although Apple is praised for its strong stance on user privacy, it has been criticised for limiting third-party developers from building more robust parental control features through restrictive sandboxing practices.

6.2.1 Family filters and child safety tools

A robust approach to child online safety requires protective measures at all levels of the technology stack.

Family filters are essential tools for protecting children, particularly younger users, from exposure to pornography and other harmful content online. While not eliminating risk, they are effective at reducing accidental exposure through search engine results or in-game advertisements. As children grow older and become more technologically savvy, the effectiveness of family filters decreases. Teenagers often learn from peers how to bypass controls using VPNs, proxy servers, or alternate browsers.

Many New Zealand internet service providers (ISPs) offer family filtering services either directly through the network or via hardware such as routers. Network-level filtering is advantageous as it applies to all devices connected to a home's Wi-Fi network, offering a baseline level of protection without requiring configuration on individual devices. However, this form of filtering becomes ineffective when devices leave the home network, such as smartphones used on mobile data. Therefore, device-level protections remain necessary for comprehensive coverage.

It is also important to note that no current New Zealand standard or regulatory framework exists to evaluate the efficacy of these filters. There is limited transparency around how well they block harmful content, including pornography and other forms of illegal or inappropriate material.

Tech safety for parents could be simplified using a 'one product' approach such as:

- child-safe phone plans with built-in filtering and app approvals
- dual internet networks (filtered for kids, unfiltered for adults)
- certified child-safe devices clearly labelled and explained.

CASE STUDY: THE SAFE SURFER X SAMSUNG KID-SAFE SMARTPHONE

In 2024, Safe Surfer launched the Safe Surfer x Samsung Kid-Safe Smartphone in New Zealand. Designed with 'Safety by Design' principles in mind, this smartphone is the result of a successful collaboration between a global technology manufacturer and a local online safety provider and delivers a multi-layered safety approach.

Built on Samsung's Knox security platform, the device is pre-configured to disable web browsers and restrict access to the Google Play Store out of the box. This solution can be applied to any Samsung phone or tablet in New Zealand, representing a scalable model for device-level safety by design.



6.2.2 School filters

In New Zealand, content filtering for schools is provided through the Crown initiative called Network for Learning (N4L).

An estimated 95% of New Zealand schools use N4L to protect their networks. N4L has recently chosen to transition to 2degrees as their main internet provider and to Palo Alto Networks for content filtering and protection. N4L plans to transition all New Zealand schools in 2025. It is unknown yet if the quality of content filtering and protection will improve with the transition.

There is tension currently with interoperability between parental controls which are installed on home devices and school networks resulting in difficulties in getting them to work together. It's important to note that filtering technologies are not effective against content shared via the dark web, which uses encrypted communication methods and requires specialised browsers such as Tor Browser.

6.2.3 Age assurance

Age assurance is a set of technologies and methods which are used to determine a person's age.

Age estimation measures an approximate age or age range without verified sources, and age verification determines a person's age to a high level of certainty.

Apple announced an age assurance model for Apple products in 2025. The Apple approach uses age estimation and is voluntary for tech platforms. No announcement has yet been made by Google and the rest of the tech industry. Meta and other social media platforms have suggested that app stores are the best place to check for age assurance.

Some regulators are investigating more robust age verification pilots and rollouts. As part of the social media age restriction for under-16s in Australia, the government there agreed to complete a trial with age verification technology. The Age Verification Pilot will produce a report in June 2025. Following the pilot, age-restriction legislation is set to be introduced in December 2025.

Age verification technology is still emerging and appears promising, but as of yet there are only a few large-scale implementations globally.

The Australian trial will provide further information about:

- the accuracy and effectiveness of age gating, assurance, and verification technologies
- the degree of privacy preservation, including what personally identifiable information may be surfaced, when, and to what extent.

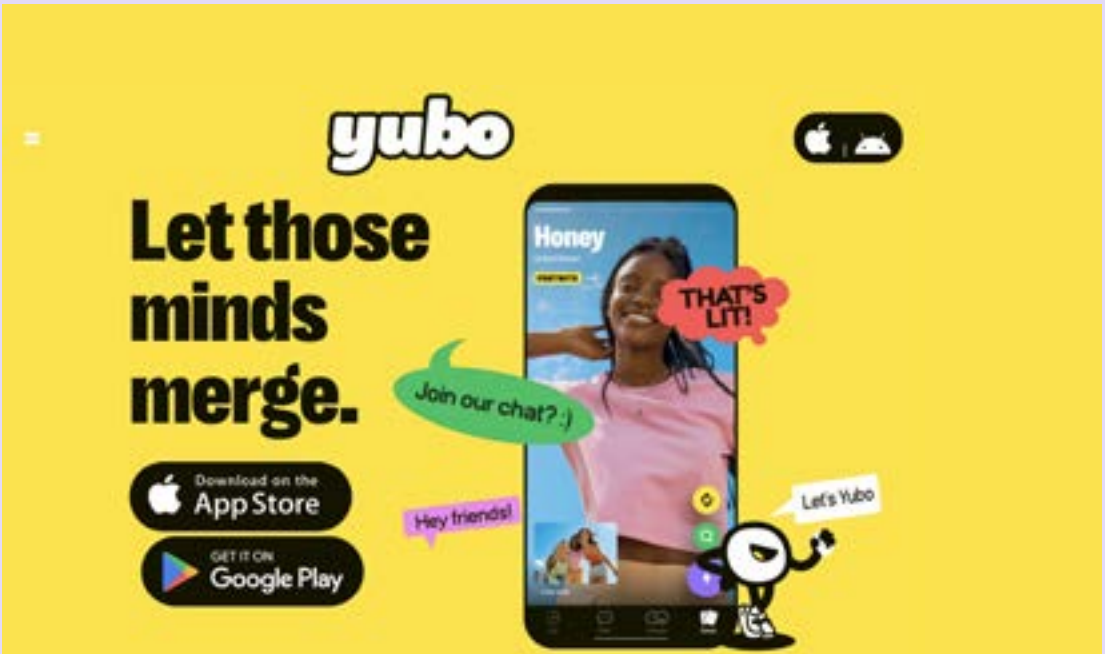
Pseudonymity and anonymity are important protective factors on the internet, particularly in some countries, and any implementation of age verification technology must be tested for factors that could affect freedom of speech.

CASE STUDY: YUBO

Yubo is a social discovery app with similarities to Snapchat. The company behind it claims Yubo is the first major social platform to age-verify that 100% of its 60 million active users are over 13 years old.

According to co-founder and CEO Sacha Lazimi, “We’ve discovered that age assurance isn’t just about mitigating safety risks – it’s a powerful tool for building trust among users, a critical second-order effect of what’s typically categorized primarily as a safety measure.”

Lazimi (2025) notes that in a recent poll of more than 10,000 Yubo users, 79% reported feeling safer on Yubo compared to other platforms due to our verification requirements. More than 60% said age verification positively impacted their overall experience, while 53% indicated increased trust that they’re interacting with real people.



6.3 SAFETY BY DESIGN

Considerations at the design and conception phase by tech companies can address potential future harm.

The Safety by Design principles, developed by the Australian eSafety Commissioner in 2018, provide a foundational approach to integrating safety considerations into the design and development of digital products and services. (eSafety Australia, 2025).

Safety by Design was implemented after consultation with the industry, non-governmental organisations, advocates, parents and young people in Australia. Since 2018, Safety by Design has become a global standard with a range of different implementations. The original core principles have been regrouped into seven main recommendation groupings; these are described individually below (OECD, 2022).

6.3.1 Integrate safety considerations at the outset

Safety features should be embedded in the design phase of product development, rather than retrofitted after issues arise.

For example, build in safety features alongside main feature releases, such as limiting contact interactions with content moderation, muting, and blocking when messaging features are released. The safety considerations vary greatly depending on the audience: Are they designed for children, a mix of children and adults, or adult use only?

6.3.2 Accountability and transparency

Companies must publish clear information regarding their safety policies and the effectiveness of their safety features.

This should include regular audits and assessments of their practices to ensure compliance with safety standards.

6.3.3 Age-appropriate design

Age-appropriate design is about designing spaces that are appropriate for children in their different age groupings.

The design should include clear, accessible, and age appropriate information about the risks associated with digital services and how children can protect themselves.

6.3.4 Default safe settings

Platforms should be designed with default safety settings that minimise exposure to harmful content. For example, features that allow for user interaction should be turned off by default for child accounts.

6.3.5 Better reporting mechanisms

Children and parents should be able to report harmful content or interactions easily. Ensure that these reports are addressed promptly and effectively.

6.3.6 Child-centred design

Adopt a child-centred design approach that prioritises child development, including the evolving needs and safety of children. This includes involving children in the design process to ensure that their perspectives and experiences are considered.

6.3.7 Privacy protections

Implement privacy-by-design principles to safeguard children's data. Clear privacy settings should be provided, allowing users to control their information and understand how it is used. Specific privacy settings can be included to stop offenders gaining access to children (OECD, 2022).

6.4 FURTHER INVESTMENT NEEDED IN RESEARCH & DEVELOPMENT

The international landscape of technology interventions for preventing online sexual harm is dynamic and evolving.

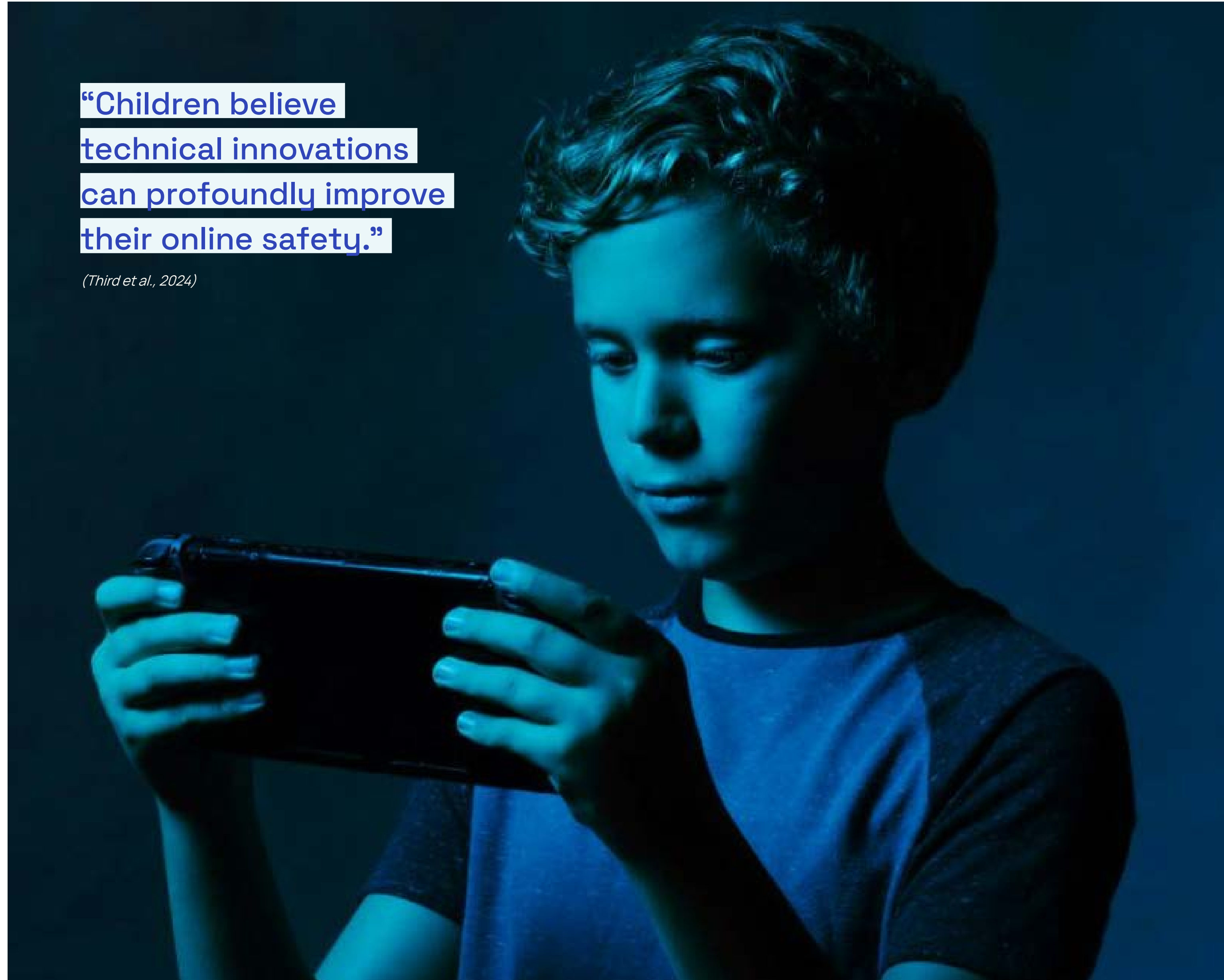
The advancements in AI for online safety present a valuable opportunity to prevent harm proactively.

Investment in new research and development into tools designed to detect AI-generated child sexual abuse material (CSAM) and deep fakes as well as innovation and collaboration between local universities, research institutions, and private sector partnerships alongside leveraging existing initiatives like IWF and C3P would speed the development of AI technologies to combat sextortion, online grooming, CSAM and help already stretched law enforcement efforts.

Investment in a dashboard which includes real-time insights into reported incidents of online harm would alert parents, educators, and industry of emerging risks and trends.

“Children believe
technical innovations
can profoundly improve
their online safety.”

(Third et al., 2024)





7

Recommendations

As young people engage across an increasingly diverse range of platforms, our societal response must evolve to reflect this complexity.

Our children and young people are exposed to ever-increasing risk of sexual harm online. At present, Aotearoa New Zealand is failing to meet its obligations under the United Nations Convention on the Rights of the Child to uphold children's rights in the digital environment (UNROC, 2021). These recommendations seek to rectify this so that children and young people can navigate the internet safely in the future.

To effectively reduce the four key online risks faced by children – Contact, Content, Conduct, and Contract – a coordinated, multi-level strategic approach is essential.

The comparative study of the institutional, governance, and government-led programmes Australia, the United Kingdom, Canada and the European Union carried out in Section 6 informs our key recommendations, which we present in this section.

Each of these have dedicated national strategies to address online harm. The World Economic Forum (2025) Roadmap to Effective Digital Safety Measures report urges a shift to prevention, with “online harm treated like a disease”, (WEF, 2025). In New Zealand, advocacy continues for an independent, robust regulatory framework aligned with international standards to protect children online (DIA, 2023; RNZ, 2024).

The recommendations and structure draw from the ACC Te Tiriti-led Primary Prevention Systems Model, ensuring a culturally grounded, systems-based approach.

“If companies can’t make online spaces safe for children, then they shouldn’t be in them.”

(Children’s Commissioner of England, 2025)

7.1 SYSTEM, LEADERSHIP, AND LEARNING

- Stewardship & advocacy / Ngā Kaitiaki
- Legislation and policy reform / Ngā Ture
- Research, Monitoring and Evaluation / Te Mahi Rangahau

7.1.1 Stewardship and advocacy / Ngā Kaitiaki

The process of reform should begin with broad consultation with key stakeholder groups, honouring Te Tiriti o Waitangi obligations through co-design with Māori and ensuring adequate Māori representation in all levels of leadership and delivery.

This work was started by the Safer Online Services and Media Platforms (SOSMP) review, which provides a solid foundation for this consultation process.

Broad stakeholder engagement is necessary and should include:

- tech platforms (Meta, Google, TikTok, Discord, Pornhub, etc.)
- Internet Service Providers (ISPs)
- non-governmental organisations and advocacy groups (e.g., Safeguarding Children, Save the Children, Rape Prevention Education)
- youth (e.g., Whāraurau youth advisors, Rainbow Youth, VOYCE)
- education providers (Netsafe, N4L, The Light Project)
- community representatives and free speech advocates
- health professionals and researchers in child wellbeing, trauma, and digital safety.

Stakeholder engagement should be nationally representative, including feedback from priority groups such as LGBTQIA+, religious groups and ethnic groups.

7.1.2 Legislation and policy reform / Ngā Ture

The development of a collaborative, legislated regulatory framework; integrating policy, education, and industry responsibility, that offers stronger protection from online harm. The current voluntary approach is not effective.

From the foregoing analysis of the digital sexual landscape and young people in Aotearoa, we recommend four key pillars for reform:

1. Develop and publish a **National Strategy to Address Online Child Sexual Abuse and Harm**. This would require a multi-agency, whole-of-society approach to ensure its effectiveness.
2. Develop a comprehensive **Children's Online Safety Act** to establish a clear legal framework for online child protection.
3. Establish a **Children's Online Commissioner** to lead and oversee enforcement and advocacy and maintain a strong regulatory framework to protect children and young people from harmful online exposure.

4. Establish a **Centre for Children's Online Safety** as a dedicated national agency for children's online safety leading strategy, education and coordination, led by a Minister of Children's Online Safety. The Centre would bring together all key stakeholders, including agencies, educators, tech firms, child protection experts, and families. It would also promote digital literacy and safety education in schools and homes, empowering parents and teachers to guide children's online activity. The Centre would encourage international collaboration through multi-lateral forums such as OECD and UN bodies to align global standards and share best practices.

“The Proposal must have a significant Māori presence within all levels of the regulatory body to comply with Te Tiriti o Waitangi obligations.”

(Mental Health and Wellbeing Commission, 2023)

“Coordination and collaboration between stakeholders and international partners are important aspects of addressing online [child sexual exploitation].”

(Public Safety Canada, 2022)

These four pillars are described in detail below.

1. DEVELOP A NATIONAL STRATEGY TO ADDRESS ONLINE CHILD SEXUAL ABUSE AND HARM

UNICEF, the OECD, WeProtect Global Alliance, the National Coalition to Prevent Child Sexual Abuse and Exploitation (also known as Prevent Together, an advisory group of the US National Center for Missing and Exploited Children) all recommend standalone, national digital child protection strategies grounded in children's rights and designed to proactively address emerging online risks. This should be led by government, supported by a cross-agency approach and overseen and managed by a **Centre for Children's Online Safety**.

A new national strategy is clearly required. It is important to note that the scope of Te Aorerekura: National Strategy to Eliminate Family Violence and Sexual Violence is not digital-specific: it takes a strengths-based and whānau-centred (community-led) approach. It is not focused on technology regulation, age verification, industry accountability, online exploitation trends, or digital public health measures. Key departments, commissioners and Crown entities who focus on online harm and enforce regulation – DIA, the Classification Office, Customs, Netsafe, and the Children's Commissioner – are missing from the strategic direction set by Te Puni Aonui.

2. DEVELOP A COMPREHENSIVE CHILDREN'S ONLINE SAFETY ACT TO ESTABLISH A CLEAR LEGAL FRAMEWORK FOR ONLINE CHILD PROTECTION

The Films, Videos, and Publications Classification Act 1993 is not fit for purpose in today's online environment. A legislated Children's Online Safety Act would establish a clear legal framework for online child protection, setting mandatory safety standards for digital platforms, internet service providers, and device manufacturers, while ensuring accountability in the digital space (WeProtect Global Alliance, 2024).

“Advertising and harmful content are top concerns, with more than 750 children [in a sample of 1,000] calling for greater control over ads and stronger protection from harmful material.”

(Save the Children & Netsafe, 2025)

Drawing on recommendations from the **Classification Office's (2023) SOSMP review submission** and aligned with international best practice, we support the inclusion of the following components in a Children's Online Safety Act:

a) The Act should introduce a code-based regulatory system tailored to each part of the online ecosystem, developed with industry bodies and expert steering groups.

This would include the following:

- a **Social Media Services Code** (e.g., Facebook, Instagram, TikTok)
- an **App Distribution Services Code** for app distribution services used to download apps (e.g., Apple iOS, Google Play)
- a **Hosting Services Code** (e.g., Amazon Web Services, Google Cloud)
- an **Internet Carriage Services Code** (e.g., Spark, Vodafone, Vocus)
- an **Equipment Code** for manufacturers, suppliers, and installers of internet-connected devices (e.g., modems, smart TVs, phones, tablets, e-readers)

b) The Act should stipulate clear and enforceable content regulation requiring platforms to proactively detect, remove, and prevent child sexual exploitation material and other harmful content, including the use of AI.

The regulatory framework should clearly define and classify specific forms of harmful content as an essential starting point. This includes clear classification of objectionable content: Terms like 'forced porn' should be explicitly illegal, ensuring legal clarity around exploitative content. The Act should also require consistent enforcement across platforms and regulate the role of algorithms, especially those that amplify harmful content or increase risk to young people.

c) The Act should:

- introduce stronger enforcement powers for regulators, including penalties for non-compliance
- retain legally enforceable age restrictions for certain types of content and platforms
- implement an industry levy to fund public awareness campaigns and harm prevention initiatives
- establish national filtering standards.

d) With regard to age verification and access controls:

- Robust age verification should be required for high-risk platforms and app stores, especially to restrict access to pornography and other adult content. Age verification technology is still emerging, with only a few large-scale implementations globally. New Zealand has a valuable opportunity to observe and learn from Australia's trial and should scope a small, locally led project to assess whether such technology is fit for purpose in the Aotearoa context. The principle of double anonymity (privacy-preserving) is also important here.
- Age assurance legislation should be supported at the app store level to prevent underage access.
- 'Nudify' apps and other non-consensual technologies are inherently harmful and should be disallowed.

e) A user-friendly, accessible complaints process should be established by the Act following a 'one front door' or 'no wrong door' approach (Classification Office, 2023). Users must be able to easily report harmful content or breaches, with clearly defined outcomes and timelines. Annual transparency reporting that tracks how platforms address complaints and harmful content should also be included.

f) The Act should also establish minimum national safety standards for school devices, online learning, and school-based internet and filtering.

g) Finally, there will need to be clear separation between the regulator and censorship functions (Classification Office, 2023) to maintain public trust and regulatory integrity. The regulator should operate transparently and independently, free from political or commercial influence.

Additionally, the following legislative gaps need to be addressed:

- Legislation needs to be established to address technology-facilitated sexual violence, sextortion and image-based abuse.
- The Harmful Digital Communications Act 2015 currently has limited ability to criminalise deepfake abuse because “intent to cause harm” is required. This effectively prioritises the harm over the victim.
- Law enforcement agencies need to be equipped to handle these cases sensitively and effectively with robust and ongoing workplace training (Wolbers et al., 2025).

“It is clear that the system as it currently operates does its best to tackle online harm, but is imperfect ...It is designed to be reactive and focuses on seeking to remedy harm only once it has occurred. Current legislation does not oblige platforms, nor indeed any other actors, to take proactive measures to reduce or prevent online harm.”

(Netsafe response to the Safer Online Services and Media Platforms Consultation, 2023)

3. ESTABLISH A CHILDREN’S ONLINE COMMISSIONER

We propose the creation of an ‘Online Children’s Commissioner’ to lead policy, enforcement, advocacy, and oversight of a robust regulatory framework that protects children and young people from harmful online exposure.

Experts continue to warn that industry self-regulation is insufficient amid rising online harms such as grooming, CSAM distribution, and algorithmic amplification of harmful content.

The Commissioner would function similarly to the Classification Office, with a mandate that addresses the online space. Its core functions should be:

- Support implementation and enforcement of an Online Children’s Safety Act.
- Oversee ISP filtering and platform safety.
- Regulate child-targeted online commerce and advertising.
- Monitor and report on compliance across digital platforms.

- Enforce penalties for breaches, including illegal content and unsafe design.
- Ensure transparency and accountability from tech companies and service providers.
- Advocate for children's digital rights and wellbeing.
- Represent children in policy development and legislative reviews.
- Protect against censorship overreach while upholding child protection goals.

4. ESTABLISH A CENTRE FOR CHILDREN'S ONLINE SAFETY

In parallel, a dedicated national agency for children's online safety should be established to lead strategy, education, and coordination efforts.

This agency would unite key stakeholders – educators, tech platforms, child protection experts, researchers, government agencies, international organisations and families – to create a safer digital environment for children.

The Centre should function similarly to the current Crown entity Netsafe, however would need a wider mandate and should remain independent from industry.

Its core functions should be:

- Support schools with safe device and filtering policies.
- Certify child-safe devices and filters.
- Run an ISP Family Filter Certification Scheme.
- Operate a tech safety testing unit.
- Tools and campaigns for families.
- Lead digital wellbeing campaigns.
- Develop parenting education programmes.
- Support the Ministry of Education with child-centred education.

The recommended structure assigns regulation and enforcement to the Commissioner, while the Centre handles delivery, education, and industry coordination.

Refer to Comparable policy chart, Holly Brooker (5.2)

7.1.3 Research, monitoring, and evaluation / Te mahi rangahau

International best practice indicates that data are an essential part of developing a model national approach to addressing child sexual abuse.

Over three-quarters of 42 countries (83%) surveyed by Unicef (2022) had some form of national research, analysis and monitoring on child sexual exploitation and abuse, including forms facilitated by technology. Without this, countries face challenges in setting baselines and indicators, and in designing a monitoring framework for national action.

Data can be used to inform targeted interventions and policy development (Wolbers et al., 2025) and to ensure emerging trends are being responded to and young people are supported. All research should be free from direct or indirect industry funding to avoid biased, unreliable outcomes. Even with a sound methodology and reliable data, industry ties undermine public and advocate trust, diminishing the research's impact.

5.INVESTMENT IN INNOVATION IS NEEDED TO
REDUCE ONLINE-RELATED HARM

Investment in research and technological advancements will be essential to stay ahead of emerging AI threats.

Innovative solutions are needed to combat sextortion, online grooming, CSAM, AI-generated CSAM, wider objectionable content and other online-related harms. Real-time insights can inform timely interventions and policies. A dashboard could present emerging risks to inform parents, educators, and industry.

7.2 CAPABILITY AND COORDINATION

Prevention system infrastructure:

- Workforce and organisational development / Ngā Mātanga
- Coordination and partnership / Ngā Rangatira

7.2.1 Workforce and organisational development

Nationwide workforce and organisational development is recommended to build confident, skilled and well-equipped FVSV, health, youth, justice, and social services.

Workforce development should include evidence-based, foundational and specialised training and resources to guide and inform workplace prevention, assessment and response initiatives relating to the digital sexual landscape. Key components should include:

Foundational digital sexual landscape training:

Evidence-based training to improve workforce understanding of the digital sexual landscape, youth usage patterns, trends, and emerging technologies such as AI is essential. It should cover impacts and risks, including TFSV, IBA, and new sexual norms. The training should provide guidance on facilitating safe, shame-free conversations with young people, fostering online resilience, developing critical thinking, and promoting ethical digital citizenship and protective factors. It should also address specific risks for vulnerable groups, promote culturally safe approaches for rangatahi Māori, and offer information on support services and referral pathways for young people and their families.

Specialised intervention and response training:

Advanced training is recommended for specialised services with evidence-based prevention, intervention and response tools and strategies for TFSV and online-related sexual harms. This should include strategies for integrating online sexual behaviours into FVSV assessments, addressing online drivers of sexual violence, and incorporating critical thinking into primary prevention programmes. It should also cover prevention and management pathways for TFSV, IBA, PPU, and harmful experiences of rough sex and 'choking' / sexual strangulation. Additionally, it should provide tools for working with vulnerable youth and young people with harmful sexual fantasies or behaviours, along with strategies for managing early exposure to CSAM and other objectionable content.

National digital sexual landscape resources:

The development of a central suite of national resources for FVSV, health, youth, justice and social services is recommended. These should encompass evidence-based information, tools and response pathways to support sector practice, prevention and response initiatives related to the digital sexual landscape.

The resources should include:

- **Understanding the digital sexual landscape:** Data and information on platforms, pornography, trends, usage patterns, and emerging technology such as AI.
- **Understanding digital sexual risks and impacts:** Information on TFSV, IBA, and the impacts of porn and on sexual attitudes, behaviours and norms around sexual violence.
- **Primary prevention tools:** Resources to integrate into existing workplace assessment and prevention frameworks to build critical thinking, challenge harmful online norms, and strengthen protective factors.
- **Navigating safe conversations with youth:** Principles and strategies for engaging in safe and effective conversations with youth.
- **Image-based sexual harm prevention:** Tools to build youth confidence and agency online, foster critical thinking around online sexual interactions, and identify risks and red flags.
- **Resources for vulnerable young people:** Prevention and early intervention tools for youth with harmful sexual thoughts and behaviours to foster critical thinking and counter problematic online messages.
- **Support for sexuality and gender-diverse youth:** Tools to help navigate early exposure, foster resilience and critical thinking.
- **Diverse sexual behaviours, rough sex, and 'choking':** Assessment, prevention and response tools and strategies, including addressing harmful norms and risk mitigation with rough sex and non-fatal strangulation.
- **Healing and response tools for problematic porn usage (PPU):** Response strategies for PPU, escalating or evolving porn usage, and unwanted porn-related experiences.
- **Healing and response tools for TFSV and IBA:** Response pathways for IBA, including sextortion, 'revenge porn', CSAM exposure, deepfakes, unwanted nudes, and AI-generated harms.
- **Resources for parents and communities:** Information on the digital landscape, guidance for conversations, and strategies to help youth build resilience and adopt protective online behaviours.
- **Case studies:** Workplace case studies illustrating common presentations of online-related harms and assessment, prevention and management responses.

7.2.2 School/Education Workforce and Organizational Development

Nationwide workforce development is needed to build school staff knowledge, skills, and capability around the digital sexual landscape.

Schools are a key frontline service for young people experiencing online harm, and report rising harms associated with pornography, objectionable content, non-consensual nudes, shifting sexual norms, deepfakes, and other forms of TFSV. Pre-training surveys from The Light Project show significant knowledge gaps, with many staff feeling unprepared to keep pace with digital trends or respond to complex harms. **Widespread sector training is needed, including the following:**

INTRODUCTORY DIGITAL SEXUAL LANDSCAPE TRAINING (WHOLE SCHOOL)

Evidence-based training for all school staff including senior leadership, teachers, and teacher aides to improve understanding of the digital sexual landscape, youth trends, and emerging technologies. Training should cover pornography, TFSV, IBA, and shifting sexual norms, and offer guidance on facilitating safe, shame-free conversations, promoting ethical digital citizenship and protective factors, and referral pathways and support services.

SPECIALISED TRAINING FOR SCHOOL GUIDANCE COUNSELLORS

Targeted training to support assessment, intervention, and response to online-related sexual harm and TFSV. This includes the relationship between porn and sexualised media on youth attitudes and norms, alongside assessment and response strategies for TFSV, CSAM exposure, problematic porn use, and disclosures of online-related harms such as rough sex and 'choking'. It should also include referral pathways and strategies for supporting vulnerable students, including those exhibiting harmful online sexual thoughts or behaviours.

SPECIALISED TRAINING FOR HEALTH AND RSE TEACHERS

RSE teachers require in-depth training on TFSV, IBA, and the impact of porn and sexualised media on youth development, attitudes, and norms. Training should support the integration of online safety into RSE including fostering critical thinking, countering harmful messages, and identifying risks. This should be underpinned by evidence-based pedagogies such as ethical sexual citizenship, which encourage youth-centred, participatory, strengths-based learning.

This approach equips young people to be safe and ethical digital citizens, promotes online respect, deepens awareness of the social, psychological, and legal impacts of online sexual engagement - building youth sexual agency and minimising the risk of harm. Training must also include inclusive, culturally safe approaches, with guidance on supporting rainbow youth, engaging rangatahi Māori, and connecting students and whānau to referral services.

WORKFORCE DEVELOPMENT IMPLEMENTATION

In the absence of a coordinated national education response, many schools are now independently seeking support to address rising online harms. This has led to an ad hoc and often ineffective approach, with some training lacking an evidence base, omitting prevention and support pathways, or focusing narrowly on staff or parents. As a result, schools have reported feeling overwhelmed and underprepared. **Effective, school-based workforce development should include:**

- A whole-of-school approach, engaging leadership, staff, parents, and wider communities.
- Safe and tailored delivery, recognising many schools communities' preference for face-to-face engagement on sensitive topics.

- Partnerships with school community, faith, and cultural groups, ensuring inclusive and culturally safe practice.
- Flexible, responsive training that can be updated and allow for real-time questions and discussion. Schools report these are more effective and better received than static online modules that can rapidly outdate.
- Evidence-based prevention grounded in ethical sexual citizenship pedagogy and supported by Aotearoa-based research.
- Clear early intervention and response pathways.
- Local referral and support services.

7.3 ACTION IN THE COMMUNITY

Prevention system infrastructure:

- Direct Participant Programmes / Ngā Wānanga
- Community mobilisation / Te Whakaoreore Hapori
- Behaviour change communications / Ngā mahi a te rēhia

Behaviour change refers to the process of shifting individuals' actions, habits or decision-making patterns. Core elements are Awareness, Motivation, Capability, and Opportunity. It involves delivering targeted messages through various channels (such as peer interactions, group settings, and mass media) to support positive behavioural shifts. Recognising that meaningful change takes time, BCC relies on sustained, coordinated efforts across multiple stakeholders and levels of influence.

“If we don’t act now to keep up with rapid changes in how kids use technology, the mental health and wellbeing of an entire generation is at stake.”

(Common Sense Media, 2023)

7.3.1 Education for young people

While policy, national strategy, parents and caregivers bear the responsibility for child protection, education has a vital role to play. School-based programs should equip children aged 7+ with the knowledge and skills to navigate online risks like AI, sextortion, grooming, and IBA, while also addressing harmful social norms that contribute to gender-based violence.

Early, repeated exposure – 6–15 times depending on age and complexity – is critical for adopting safety concepts such as consent, privacy, and recognising online manipulation. Interactive methods like role-play, and personal stories, combined with spaced repetition and parental reinforcement, significantly boost retention.

At the same time, teaching empathy and relationship skills can counteract societal norms that normalise objectification and unrealistic expectations, particularly in boys exposed to coercive or violent male role models. Such exposure is linked to increased risk of perpetrating intimate partner violence, highlighting the need for preventative education that integrates online safety with gender-aware, trauma-informed approaches.

For adolescents in particular, embedding ethical digital and sexual citizenship education approaches that promote critical thinking, empathy, respectful engagement, and an understanding of the social, psychological and legal impacts of online behaviour is paramount. This strengths-based approach can help counter harmful online sexual norms, foster agency and resilience, and offer effective protection from the influence of porn on attitudes and beliefs around violence.

[Te Puna Aonui has already developed resources ready for an RSE refresh](#), due to the scope of this report, we have not reported on the content of those resources.

7.3.2 Public campaigns and parent education

A nationwide campaign should target parents and caregivers across all age groups, emphasising the importance of prevention and response to harm. It should be led by the recommended Centre for Children's Online Safety. The campaign should include clear, age-based guidelines for when and how to introduce devices and educate parents on the risks of early digital exposure, safer alternatives, and strategies for managing technology. As digital trends rapidly evolve e.g. the rise of AI companions, parents face growing blind spots that leave children and young people vulnerable. Ongoing, community-led investment in family digital literacy is essential to effective, long-term harm prevention.

To effectively reduce harm, campaigns should engage families in a way that resonates with diverse communities, including early childhood, primary, intermediate, and high schools. The success of previous public messages (e.g., New Zealand Police's statement in 2024 urging parents to be more vigilant) has been impactful. Authoritative, urgent messaging can drive immediate action. Research indicates mothers are more likely to discuss online safety but wider targeting is essential for creating long-term cultural change. Interventions should address the roles of all parents and caregivers to ensure consistent online safety practices across households, particularly when children split time between homes.

Practical interventions can be modelled off health campaigns. A safety campaign could involve distributing informational leaflets with fridge magnets, modelled after Healthline's antenatal resources, offering online safety strategies and helplines. This method ensures accessibility for all households, including those with limited digital literacy. Physical materials encourage ongoing engagement and serve as constant reminders, unlike websites which are often accessed by adults only after harm has occurred.

Supporting campaigns, practical parenting courses and online resources should be rolled out nationwide, particularly when a new trend emerges.

7.3.3 Social norms around internet and device use

Currently the social norms of internet and smartphone use, such as early ownership of devices, unrestricted access to apps, and having devices in bedrooms, are not cautious enough given the risks of online sexual harm.

Keeping school devices on-site until high school can help shift social norms around children's device use by reinforcing the idea that digital access is for learning, not constant personal use. It reduces children's access to private, unsupervised devices at home and lessens reliance on parental controls alone. Many parents are unaware that school filtering systems do not apply once devices are used off-site, making on-site-only policies an important safeguard.

Reducing online harm may be linked to socioeconomic factors, with lower-income youth spending up to twice as much time on screens. Engaging less online often reflects access to structured alternatives, like sports or hobbies, which build resilience, reduce risk, build protective social networks, and displace risky behaviours. Investment in after school activities on school premises would significantly reduce screen time and in turn exposure to harm (Centers for Disease Control, 2005; Common Sense Media, 2019; PMC, 2013; Science Direct, 2022; Women's Sports Foundation, 2009).

7.3.4 Media industry collaboration and content warnings

Implementing a warning system for mainstream media content, such as tagging episodes with warnings like “This episode shows sexual content that may be illegal or fatal if tried in real life” (e.g., for depictions of ‘choking’ / strangulation). Broadcasters and streaming platforms could integrate warnings for specific high-risk themes. The point would be to enhance viewer awareness, reduce unintended normalisation of dangerous behaviours, and potentially mitigate ethical liabilities for platforms. However, applying this universally across all shows might overwhelm audiences with warnings, diluting their impact and creating logistical challenges. A more practical approach could target emerging issues, such as rising trends in risky behaviour tied to media, allowing for focused warnings where data shows a real need, rather than a blanket policy that risks desensitising viewers or requires heavy resourcing.

7.3.5 Tailored support for minority groups

When designing online safety campaigns and interventions, it is essential to consider the specific needs and experiences of minority groups who may face heightened risks or barriers to support. **Key groups to consider include:**

- 1. Māori and Pasifika communities:** These communities may have different cultural norms around parenting, digital access, and trust in institutions. Culturally tailored, community-led approaches are essential.
- 2. Rainbow/LGBTQIA+ youth:** These young people often turn to online spaces for identity exploration and community but are at higher risk of online harassment, grooming and exploitation.
- 3. Children with disabilities or neurodivergence:** These groups are more vulnerable to online manipulation, exploitation and cyberbullying due to communication challenges, emotional dysregulation, impulsivity, and social isolation.
- 4. Migrant and refugee families:** Language barriers, unfamiliarity with local digital norms, and lower trust in authorities can reduce access to online safety information and support.

5. Low-income families: Children in these households often spend more time online and may have unsupervised access due to parental work demands or limited access to structured activities.

6. Children in shared-care or separated families: Inconsistent online safety rules and device monitoring between households can increase vulnerability.

7. Rural or remote communities: These families may experience limited access to digital literacy resources, support services, or reliable internet, which affects both access to help and risk exposure.

References

Acres, T. (2023, October 23). What is the Online Safety Bill, who is in favour, who opposes it, and how will it be enforced? Sky News.
<https://news.sky.com/story/what-is-the-online-safety-bill-who-is-in-favour-who-opposes-it-and-how-will-it-be-enforced-12964247>

ACT New Zealand. (n.d.). Defending freedom of expression. <https://www.act.org.nz/defending-freedom-of-expression>

ACT Party. (2024). Deepfake, digital harm and exploitation bill (Version 1.3).https://assets.nationbuilder.com/actnz/mailings/23487/attachments/original/Deepfake_Digital_Harm_and_Exploitation_Bill-v1.3.pdf?1746845179

Akin Gump Strauss Hauer & Feld LLP. (2023, January 25). California deepfake laws: First in country to take effect [Blog post].
<https://www.akingump.com/en/insights/blogs/ag-data-dive/california-deepfake-laws-first-in-country-to-take-effect>

American Psychological Association. (2021). Understanding trauma and its impact. <https://www.apa.org/topics/trauma>

Argentino, M. A., Barrett, G., & Tyler, M.-B. (2024, January 19). 764: The intersection of terrorism, violent extremism, and child sexual exploitation.

Australian Centre to Counter Child Exploitation. (n.d.). About the ACCCE. <https://www.accce.gov.au/what-we-do/about-us>

Australian Centre to Counter Child Exploitation. (n.d.). ACCCE statistics.<https://www.accce.gov.au/resources/research-and-statistics/statistics>

Australian Federal Police. (2024, March 30). Tasmanian jailed for possessing AI-generated child abuse material [Media release].
<https://www.afp.gov.au/news-centre/media-release/tasmanian-jailed-possessing-ai-generated-child-abuse-material>

Australian Institute of Family Studies. (2020). Trauma-informed care in child/family welfare services. <https://aifs.gov.au/resources/policy-and-practice-papers/trauma-informed-care-childfamily-welfare-services>

Australian Institute of Family Studies. (2021). Longitudinal Study of Australian Children: Annual statistical report 2021.
<https://aifs.gov.au/growing-australia/corporate/longitudinal-study-australian-children-annual-statistical-report-2018>

Australian Institute of Criminology. (2021, September). Cyber strategies used to combat child sexual abuse material (Trends & Issues in Crime and Criminal Justice No. 636). Australian Government.
https://www.aic.gov.au/sites/default/files/2021-09/ti636_cyber_strategies_used_to_combat_csam.pdf

Australian Online Safety. (2024). Online safety codes. Australian Government. <https://onlinesafety.org.au>

Baker, G. (2023, April 4). The EU Digital Services Act: A win for transparency. Freedom House. <https://freedomhouse.org/article/eu-digital-services-act-win-transparency>

Barker-Clarke, E. (2023). Girls Navigating the Context of Unwanted Dick Pics: 'Some Things Just Can't Be Unseen'. <https://doi.org/10.3390/youth3030060>

Bailey, A., Findlater, D., Wortley, R., & Zuhair, D. (2024). Accessing child sexual abuse material: Pathways to offending and o. Child Abuse & Neglect. <https://doi.org/10.1016/j.chiabu.2024.106936>

Barlett, H. (2024, October 1). Man sentenced in Tauranga for child sexual abuse and exploitation material. New Zealand Herald.
<https://www.nzherald.co.nz/nz/man-sentenced-in-tauranga-for-child-sexual-abuse-and-exploitation-material/WOMT4MHLS5GD5BF77EOBYXHWK4>

Barrett, E., Pettifer, S., Marsh, J., Flynn, S., Turner, P., & Hill, K. (2022). Intelligence briefing: Extended reality technologies and child sexual exploitation and abuse. The University of Manchester & WeProtect.

BBC News. (2023, November 7). Instagram: Meta whistleblower says platform not safe for kids. <https://www.bbc.com/news/technology-67343550>

BBFC. (2022). Research on animated content and its impact on perceptions of abusive relationships. British Board of Film Classification.

Bell Gully. (2024). A balancing act: Achieving safer online services and media platforms. <https://www.bellgully.com/insights/a-balancing-act-achieving-safer-online-services-and-media-platforms/>

Benford, Criscillia and Rachel Franz. (2025, February). "Buying to Belong: Youth and Virtual Assets in the Metaverse." Fairplay. <https://fairplayforkids.org/pf/buyingtobelong>

Bharadwaj, A. (2024, August 24). Online safety watchdog warns of sex chat bots targeting Australian kids. Daily Telegraph. <https://www.dailytelegraph.com.au/news/online-safety-watchdog-warns-of-sex-chat-bots-targeting-australian-kids/news-story/ebd149cb35a5c6659cfbe1e2ff49a8e4>

Bing. (2024). Search engine results data for objectionable content. <https://www.bing.com>

Bloxsom G, McKibbin G, Humphreys C, Davidson J, & Halfpenny N. (2024). Five Forms of Coerced "Self-Produced" Child Sexual Exploitation Material: A Critical Interpretive Synthesis. Trauma Violence & Abuse. doi: 10.1177/15248380241271376

Boniel-Nissim, M., Marino, C., Galeotti, T., Blinka, L., Ozoliņa, K., et al. (2024). A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey. World Health Organization. <https://iris.who.int/handle/10665/378982>

Bonobology. (2023, August 2). Teenage dating apps – 11 dating apps for under 18. Bonobology. <https://www.bonobology.com/dating-apps-for-teens/>

Boughen, B. (2023, April 3). Civil society groups band together to 'Fix the Code'. Tohatoha.

Bradley, K. (2017, October 11). Making Britain the safest place in the world to be online [Press release]. GOV.UK. <https://www.gov.uk/government/news/making-britain-the-safest-place-in-the-world-to-be-online>

Bridges, A. J., Wosnitzer, R., Scharrer, E., Sun, C., & Liberman, R. (2010). Aggression and sexual behavior in best-selling pornography videos: A content analysis update. Violence against women, 16(10), 1065-1085.

British Board of Film Classification, & Revealing Reality. (2020). Young people, pornography & age-verification.

British Journal of Criminology. (2021). Sexual violence as a sexual script in mainstream online pornography. Report No. 61, Issue 5.

Byte Back Law. (2024, March). Utah legislature repeals and replaces Utah Social Media Regulation Act. <https://www.bytebacklaw.com/2024/03/utah-legislature-repeals-and-replaces-utah-social-media-regulation-act/>

Cairney, P. (2019). Understanding public policy: Theories and issues. <https://paulcairney.wordpress.com/wp-content/uploads/2019/03/chapter-12-policy-transfer-learning-upp-2nd-ed-9.3.19.pdf>

Calvete, E., Orue, I., and Gámez-Guadi, M. (2022). A Preventive Intervention to Reduce Risk of Online Grooming Among Adolescents. Psychosocial Intervention, 31(3), 177 - 184. <https://doi.org/10.5093/pi2022a14>

Canadian Centre for Child Protection. (n.d.). Protect children. <https://www.protectchildren.ca/en/>

Canadian Centre for Child Protection. (n.d.). Protect children. <https://www.protectchildren.ca/en/>

Centers for Disease Control and Prevention. (2023). National Health Interview Survey–Teen, 2021–2023. https://www.cdc.gov/nchs/nhis/teen/?CDC_AAref_Val=https://www.cdc.gov/nchs/nhis/teen.htm

Centre of Expertise on Child Sexual Abuse, 2023, Key messages from research on children and young people who display harmful sexual behaviour.

Chen, L., & Shi, J. (2019). Reducing harm from media: A meta-analysis of parental mediation. *Journalism & Mass Communication Quarterly*, 96(1), 173–193. <https://doi.org/10.1177/1077699018754908>

Cheyne, C., & Hambleton, R. (2011). The Kiwi connection: Reflections on local governance policy transfer between the UK and New Zealand. *Journal of Comparative Policy Analysis*, 13(2), 215–231. <https://doi.org/10.1080/13876988.2011.556000>

Children's Commissioner for England, 2023, "A lot of it is actually just abuse ": Young people and pornography. <https://www.childrenscommissioner.gov.uk/resource/a-lot-of-it-is-actually-just-abuse-young-people-and-pornography/>

Christenson, P., Fox, J., & Joffe, A. (2020). The impact of ongoing victimization through circulation of child sexual abuse material. *Journal of Child Sexual Abuse*, 29(5), 567–582.

Children's Commissioner for England, 2023, "A lot of it is actually just abuse ": Young people and pornography.

Children's National Advocacy Network Ireland. (n.d.). Online safety framework. <https://www.cnam.ie/general-public/online-safety/online-safety-framework/>

Chin-Rothmann, C., Rajic, T., & Brown, E. (2023, October 18). A new chapter in content moderation: Unpacking the UK Online Safety Bill. CSIS. <https://www.csis.org/analysis/new-chapter-content-moderation-unpacking-uk-online-safety-bill>

Christenson, L., & Tsagaris, T. (2020). Offenders convicted of child sexual exploitation material offences: Characteristics of offenders and an exploration of judicial censure. *Psychiatry, Psychology and Law*. <https://doi.org/10.1080/13218719.2020.1742240>

Clarkson, S., & Kirwin, E. (2024, October 17). Social media face big changes under new Ofcom rules. BBC News. <https://www.bbc.com/news/articles/cj0467e9e43o>

Classification Office - Te Mana Whakaatu. (2018). NZ Youth and Porn: Research findings of a survey on how and why young New Zealanders view online pornography. https://www.classificationoffice.govt.nz/media/documents/NZ_Youth_and_Porn.pdf

Classification Office - Te Mana Whakaatu. (2019). Breaking Down Porn. A Classification Office Analysis of Commonly Viewed Pornography in NZ (2019). https://www.classificationoffice.govt.nz/media/documents/Breaking_Down_Porn.pdf

Classification Office - Te Mana Whakaatu. (2020). Getting real about the impacts of online pornography on young people. <https://www.beehive.govt.nz/sites/default/files/2020-12/Classification%20Office-4.pdf>

Classification Office - Te Mana Whakaatu. (2023, July). Submission on the Safer Online Services and Media Platforms public consultation. https://www.classificationoffice.govt.nz/media/documents/20230731_Submission.pdf

Classification Office - Te Mana Whakaatu. (2024). Content that Crosses the Line: Conversations with young people about extremely harmful content online. Wellington, NZ.

https://www.classificationoffice.govt.nz/media/documents/Classification_Office_-_Content_that_Crosses_the_Line.pdf

Coimisiun na Mean. (n.d.). Online safety. <https://www.cnam.ie/online-safety>

Collier, A. (2019, January 16). 7 Great Developments in Internet Safety That Happened in 2018. London School of Economics and Political Science.

<https://blogs.lse.ac.uk/parenting4digitalfuture/2019/01/16/7-great-developments-in-internet-safety-that-happened-in-2018/>

Common Sense Media. (2019). Media use by Tweens and Teens.

<https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2019>

Conte, J. R. (2024). Introduction to Special Section: Developing a National Strategy to Prevent and End Child Sexual Abuse. *Journal of Child Sexual Abuse*, 33(7), 825–832.

<https://doi.org/10.1080/10538712.2024.2430609>

Cornish, S., & Strang, B. (2021, November 20). Family violence case reported every four minutes, predicted to worsen. Stuff.

<https://www.stuff.co.nz/national/crime/127027234/family-violence-case-reported-every-four-minutes-predicted-to-worsen>

Counter Hate. (2021, December 30). Facebook's metaverse. <https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/>

Coyne, S. M., Ward, L. M., Kroff, S. L., Davis, E. J., Holmgren, H. G., Jensen, A. C., Erickson, S. E., & Essig, L. W. (2019). Contributions of mainstream sexual media exposure to sexual attitudes, perceived peer norms, and sexual behavior: A meta-analysis. *Journal of Adolescent Health*, 64(4), 430–436. <https://scholarsarchive.byu.edu/>

Cullen, J., Muntz, A., Marsh, S., Simmonds, L., Mayes, J., O'Neill, K., & Duncan, S. (2024). Impact of digital technologies on health and wellbeing of children and adolescents: A narrative review. *New Zealand Journal of Physiotherapy*, 52 (1), 62–77. <https://doi.org/10.15619/nzjp.v52i1.364>

D'Abreu, L. C., & Krahé, B. (2014). Predicting sexual aggression in male college students in Brazil. *Psychology of Men & Masculinity*, 15(2), 152–162. <https://doi.org/10.1037/a0032790>

Daubs, M., & Thompson, P. (2021). International regulatory frameworks for online content. Department of Internal Affairs. [https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/\\$file/International-Regulatory-Frameworks-for-Online-Content-Report.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/$file/International-Regulatory-Frameworks-for-Online-Content-Report.pdf)

Davison, I. (2018, August 10). Children's Minister Tracey Martin wants online pornography to be regulated. *New Zealand Herald*. <https://www.nzherald.co.nz/nz/childrens-minister-tracey-martin-wants-online-pornography-to-be-regulated/PQEMNUEX4WN7HZREB357HZHBDM/>

Dawson, K., Tafro, A., & Štulhofer, A. (2019). Adolescent sexual aggressiveness and pornography use: A longitudinal assessment. *Aggressive Behavior*, 45(6), 587–597. <https://doi.org/10.1002/ab.21854>

Dees, J. (n.d.). The differences between the Online Safety Act & the Digital Services Act. Trust Lab. <https://www.trustlab.com/post/the-differences-between-the-online-safety-act-the-digital-services-act>

DemandSage. (2025, January). Character AI statistics (2025) - 28 million active users. DemandSage. <https://www.demandsage.com/character-ai-statistics/>

Department for Science, Innovation and Technology. (2023, October 27). Overwhelming support for Online Safety Act as rules making UK the safest place in the world to be online become law. United Kingdom Government. <https://www.gov.uk/government/news/overwhelming-support-for-online-safety-act-as-rules-making-uk-the-safest-place-in-the-world-to-be-online-become-law>

Department of Health (UK). (2024, September 24). Domestic and sexual abuse strategy launched. United Kingdom Government. <https://www.health-ni.gov.uk/news/domestic-and-sexual-abuse-strategy-launched-0>

Department of Internal Affairs. (n.d.). Classification overview. New Zealand Government. <https://www.dia.govt.nz/Classification-Overview>

Department of Internal Affairs. (n.d.). Digital child exploitation filtering system. New Zealand Government. <https://www.dia.govt.nz/Preventing-Online-Child-Sexual-Exploitation-Digital-Child-Exploitation-Filtering-System>

Department of Internal Affairs. (n.d.). How NZ responds to online child sexual exploitation. New Zealand Government. <https://www.dia.govt.nz/Preventing-Online-Child-Sexual-Exploitation-How-NZ-responds-to-online-child-sexual-exploitation>

Department of Internal Affairs. (n.d.). Legislation and legal process. New Zealand Government. <https://www.dia.govt.nz/Preventing-Online-Child-Sexual-Exploitation-Legislation-and-legal-process>

Department of Internal Affairs. (n.d.). What is child sexual abuse material? New Zealand Government. <https://www.dia.govt.nz/Preventing-Online-Child-Sexual-Exploitation-What-is-child-sexual-abuse-material>

Department of Internal Affairs. (2022, June). Online safety experience overview. New Zealand Government. [https://www.dia.govt.nz/diawebsite.nsf/Files/digital-child-exploitation/\\$file/Online-Safety-Experience-Review.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/digital-child-exploitation/$file/Online-Safety-Experience-Review.pdf)

Department of Internal Affairs. (2023). Over 1 million access attempts blocked, and 47 investigations conducted in 2023. New Zealand Government. <https://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/e13df659ed765a7bcc258ac8006ed793!OpenDocument>

Department of Internal Affairs. (2023, April). Proactive release of Cabinet material and key advice papers relating to the release of the discussion document on modernising the regulatory framework for media and online content. New Zealand Government. [https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases-2023/\\$file/Proactive-Release-of-Cabinet-material-and-key-advice-papers-relating-to-the-release-of-discussion-document-on-modernising-the-regulatory-framework-for-media-and-online-services.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases-2023/$file/Proactive-Release-of-Cabinet-material-and-key-advice-papers-relating-to-the-release-of-discussion-document-on-modernising-the-regulatory-framework-for-media-and-online-services.pdf)

Department of Internal Affairs. (2023, March). Independent reference group meeting minutes. New Zealand Government. [https://www.dia.govt.nz/diawebsite.nsf/Files/DCEFS-Meeting-Minutes/\\$file/IRG-Meeting-Minutes-28-March-2024.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/DCEFS-Meeting-Minutes/$file/IRG-Meeting-Minutes-28-March-2024.pdf)

Department of Internal Affairs. (2024, April). Summary of submissions: Safer online services and media platforms. New Zealand Government. [https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/\\$file/Safer-Online-Services-and-Media-Platforms-Summary-of-Submissions-V2.pdf](https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/$file/Safer-Online-Services-and-Media-Platforms-Summary-of-Submissions-V2.pdf)

Department of Internal Affairs. (2024, October 1). Man sentenced in Tauranga for child sexual abuse and exploitation material. New Zealand Government.
<https://www.dia.govt.nz/Tauranga-man-sentenced-to-3-months-home-detention-for-possessing-over-8500-images-of-children-being-sexually-exploited-and-abused>

Department of Social Services. (n.d.). Ending violence. Australian Government. <https://www.dss.gov.au/ending-violence>

Department of Social Services. (2022). The National Plan to End Violence against Women and Children 2022–2032. Australian Government.
<https://www.dss.gov.au/national-plan-end-gender-based-violence/resource/national-plan-end-violence-against-women-and-children-2022-2032>

DeviantArt. (2025). Lolifetish. <https://www.deviantart.com/tag/lolifetish>

Digital Waitaha Charitable Trust. (n.d.). Research. <https://www.digitalwaitaha.org.nz/research>

Dines, G., & Sanchez, M. (2023). Hentai and the pornification of childhood: How the porn industry just made the case for regulation. *Dignity: A Journal of Analysis of Exploitation and Violence*, 8(1), Article 3. <https://doi.org/10.23860/dignity.2023.08.01.03>

Dolowitz, D., & Marsh, D. (2000). Learning from abroad: The role of policy transfer in contemporary policy-making. *Journal of Public Policy*, 11(1), 3–30. <https://doi.org/10.1017/S0143814X00004918>

Donevan, M., & Mattebo, M. (2017). The relationship between frequent pornography consumption, behaviours, and sexual preoccupation among male adolescents in Sweden. *Sexual & Reproductive Healthcare: Official Journal of the Swedish Association of Midwives*. <https://doi.org/10.1016/j.srhc.2017.04.002>

Donnell, H., & Peacock, C. (2024, May 19). Media oversight one-stop-shop stopped. Radio New Zealand.
<https://www.rnz.co.nz/national/programmes/mediawatch/audio/2018938976/media-oversight-one-stop-shop-stopped>

ECPAT. (2024). Facts and statistics. <https://www.ecpat.org.nz/facts/>

ECPAT International. (2023). Global trends in online child sexual exploitation and abuse. <https://ecpat.org>

Elmore, K. C., Scull, T. M., Malik, C. V., & Kupersmidt, J. B. (2021). Rape myth acceptance reflects perceptions of media portrayals as similar to others, but not the self. *Violence Against Women*, 27(3–4), 529–551.
<https://pmc.ncbi.nlm.nih.gov/articles/PMC7508883/>

Emery, C., Wong, P., Haden-Pawlowski, V., Pui, C., Wong, G., Kwok, S., Liu, A., & Abdullah, A. (2024). Neglect, online invasive exploitation, and childhood sexual abuse in Hong Kong: Breaking the links. *Child Abuse & Neglect*, 147, 106591. <https://doi.org/10.1016/j.chiabu.2023.106591>

Ennor, S. (2022, August 29). NZ's social media "Code of Practice" launched. Hudson Gavin Martin. <https://www.hgmlegal.com/insights/nzs-social-media-code-of-practice-launched>

eSafety. (2025, February 18). AI chatbots and companions: Risks to children and young people. Australian Government eSafety Commissioner.
<https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people>

eSafety Australia. (2025, May 1). Character.AI. Australian Government eSafety Commissioner. Retrieved March 5, 2025, from <https://www.esafety.gov.au/key-topics/esafety-guide/characterai>

eSafety Commissioner. (2021). United Nations Convention on the Rights of the Child: General Comment No. 25 (2021) Children's rights in the digital world. Australian Government.
<https://www.esafety.gov.au/newsroom/blogs/uncrc-general-comment-childrens-rights-digital-world>

eSafety Commissioner. (2023). Our legislative functions. Australian Government. <https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>

eSafety Commissioner. (2023, December). Online content scheme regulatory guidance. Australian Government.
<https://www.esafety.gov.au/sites/default/files/2023-12/Online-Content-Scheme-Regulatory-Guidance-Updated-December-2023.pdf>

eSafety Commissioner. (2024). Basic online safety expectations regulatory guidance. Australian Government.
<https://www.esafety.gov.au/sites/default/files/2024-07/Basic-Online-Safety-Expectations-regulatory-guidance-July-2024.pdf>

eSafety Commissioner. (2024, April 18). Learn about the Online Safety Act. Australian Government. <https://www.esafety.gov.au/newsroom/whats-on/online-safety-act>

European Commission. (2024). The Digital Services Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

European Union Digital Services Act. (n.d.). Home. <https://www.eu-digital-services-act.com/>

Europol. (2024). Internet organised crime threat assessment (IOCTA) 2024. <https://www.europol.europa.eu>

Europol Operations Directorate Operational and Analysis Centre. (2025, January). The rise of online cult communities dedicated to extremely violent child abuse.
<https://www.europol.europa.eu/publications-documents/rise-of-online-cult-communities-dedicated-to-extremely-violent-child-abuse>

Europol. (2022). Policing in the metaverse - What law enforcement needs to know: An observatory report from the Europol innovation lab. Publications Office of the European Union.
<https://data.europa.eu/doi/10.2813/81062>

Finkelhor, D., Turner, H., & Colburn, D. (2024). The prevalence of child sexual abuse with online sexual abuse added. *Child Abuse & Neglect*, 149, 106634. <https://doi.org/10.1016/j.chiabu.2024.106634>

Florida Senate. (2024). Senate Bill 1680 (2024). <https://www.flsenate.gov/Session/Bill/2024/1680>

Florida Senate. (2024). Senate Bill 1680 – By Version. <https://flsenate.gov/Session/Bill/2024/1680/ByVersion>

Franzen, K. (2024, October 23). Character AI clamps down following teen user suicide, but users are revolting. *VentureBeat*.
<https://venturebeat.com/ai/character-ai-clamps-down-following-teen-user-suicide-but-users-are-revolting/>

Fritz, N., Malic, V., Paul, B., & Zhou, Y. (2020). A descriptive analysis of the types, targets, and relative frequency of aggression in mainstream pornography. *Archives of Sexual Behavior*, 49(8), 3041-3053.

Fry, D. (2024, May 27). We found over 300 million young people had experienced online sexual abuse and exploitation over the course of our meta-study. *The Conversation*.
<https://theconversation.com/we-found-over-300-million-young-people-had-experienced-online-sexual-abuse-and-exploitation-over-the-course-of-our-meta-study-229039>

Frykberg, E. (2024, April 17). Former DIA worker warns thousands of children could continue to be exploited. *Stuff*.
<https://www.stuff.co.nz/nz-news/350302273/former-dia-worker-warns-thousands-children-could-continue-be-exploited-under>

- Funk, A., Weeks, H., & Radesky, J. (2020). Explaining adherence to American Academy of Pediatrics screen time recommendations with caregiver awareness and motivation. *JMIR Pediatrics and Parenting*, 3(2), e19431. <https://doi.org/10.2196/19431>
- Gallagher, B., Christmann, K., & Fraser, C. (2006). International and internet child sexual abuse and exploitation: Research report. Centre for Applied Childhood Studies. https://www.academia.edu/1168336/International_and_internet_child_sexual_abuse_and_exploitation_issues_emerging_from_research
- Gath, M., Gillon, G., McNeill, B., & Woodward, L. (2023). Assessing the impact of screen time on children's language, educational ability, and social functioning from infancy to age 8. Ministry of Social Development.
- Gerhard-Burnham, B., Underwood, L. A., Speck, K., Williams, C., Merino, C., & Crump, Y. (2016). The lived experience of the adolescent sex offender: A phenomenological case study. *Journal of Child Sexual Abuse*. 25(5), 499–518. <https://doi.org/10.1080/10538712.2016.1167803>
- Goatley, T., Wilson, K., & Cohen, A. (2023, June 28). A balancing act: Achieving safer online services and media platforms. Bell Gully. <https://www.bellgully.com/insights/a-balancing-act-achieving-safer-online-services-and-media-platforms>
- Goldbart, M. (2024, July 24). Ofcom fines TikTok nearly \$2.6M. Deadline. <https://deadline.com/2024/07/tiktok-fined-ofcom-harmful-content-1236019780/>
- Good Shepherd. (n.d.). New Zealand family violence and economic harm statistics. <https://goodshepherd.org.nz/economic-harm/new-zealand-family-violence-and-economic-harm-statistics/>
- Government Equalities Office. (2020). The relationship between pornography use and harmful sexual attitudes and behaviours: Literature review. <https://www.gov.uk/government/publications/the-relationship-between-pornography-use-and-harmful-sexual-behaviours/the-relationship-between-pornography-use-and-harmful-sexual-attitudes-and-behaviours-literature-review>
- Government of Canada. (2024). Charter statements: Bill C-63. <https://www.justice.gc.ca/eng/csj-sjc/pl/charte-charte/c63.html>
- Government of Canada. (2024). Proposed bill to address online harms. <https://www.canada.ca/en/canadian-heritage/services/online-harms.html>
- Government of Canada. (n.d.). Actions to combat online child sexual exploitation. <https://www.canada.ca>
- Gross, A., & Thomas, D. (2024, October 1). UK regulator preparing for 'strong action' against tech giants. *Financial Times*. <https://www.ft.com/content/dde817fb-3ba7-4b16-b735-3ae1ec324c4c>
- Guggisberg, M. (2024, February). Virtual reality grooming is an increasing danger. How can parents keep children safe? *The Conversation*. <https://theconversation.com/virtual-reality-grooming-is-an-increasing-danger-how-can-parents-keep-children-safe-221608>
- Haan, K. (2024, June 4). What is the Five Eyes Alliance? *Forbes*. <https://www.forbes.com/advisor/business/what-is-five-eyes/>
- Hackett, S. (2010). Children and young people with harmful sexual behaviours. In C. Barter & D. Berridge (Eds.), *Children behaving badly? Exploring children's welfare and behaviour* (pp. 121–135). Wiley-Blackwell.
- Hackett, S. (2014). *Children and young people with harmful sexual behavior*. Dartington: Research in Practice.
- Hald et al. (2013), 'Pornography and Sexist Attitudes Among Heterosexuals', *Journal of Communication*, 63(4).
- Hald, G.M., Malamuth, N.N., & Yuen, C. (2010). 'Pornography and Attitudes Supporting Violence against Women: Revisiting the Relationship in Nonexperimental Studies'. *Aggressive Behavior*, 36(1): 14-20.

Harling, A., Henesy, D., & Simmance, E. (2023, January). Transparency reporting: The UK regulatory perspective. *Journal of Online Trust and Safety*. <https://tsjournal.org/index.php/jots/article/download/108/43/320>

Harris, T. (2024, October 29). Tristian Harris warns parents of the potentially deadly consequences of AI chatbots manipulating our children. *Fox News*. <https://radio.foxnews.com/2024/10/29/tristian-harris-warns-parents-of-the-potentially-deadly-consequences-of-ai-chatbots-manipulating-our-children/>

Hedrick, A. (2021). "He's so bad but he does it so well": Interviews with One Direction fans about writing romantic and erotic fiction online. *Sex Education*, 21(4), 446–459. <https://doi.org/10.1080/14681811.2020.1829758>

Help Auckland. (2023). Sexual abuse statistics summary. <https://helpauckland.org.nz/resources/sexual-abuse-statistics-summary/>

Henry, N., Gavey, N., McGlynn, C., & Rackley, E. (2022). 'Devastating, like it broke me': Responding to image-based sexual abuse in Aotearoa New Zealand. *Criminology & Criminal Justice*, 23(5), 861-879. <https://doi.org/10.1177/17488958221097276>

Herbenick, D., Fu, T. C., Kawata, K., Eastman-Mueller, H., Guerra-Reyes, L., Rosenberg, M., & Valdivia, D. S. (2021). Non-fatal strangulation/choking during sex and its associations with mental health: findings from an undergraduate probability survey. *Journal of Sex & Marital Therapy*, 1-13.

Herbitter, C., Norris, A. L., Nelson, K. M., & Orchowski, L. M. (2022). Understanding associations between exposure to violent pornography and teen dating violence among female sexual minority high school students. *Journal of Interpersonal Violence*, 37(17–18), NP17023–NP17035. <https://doi.org/10.1177/08862605211028314>

Her Majesty's Government UK. (2021, July). Tackling violence against women and girls. UK Government. https://assets.publishing.service.gov.uk/media/6194d05bd3bf7f054f43e011/Tackling_Violence_Against_Women_and_Girls_Strategy_-_July_2021.pdf

Hern, A., & Milmo, D. (2022, July 13). Flawed online safety bill is disaster for free speech, claim Tories. *The Guardian*. <https://www.theguardian.com/technology/2022/jul/13/online-safety-bill-tories-free-speech-david-davis>

Heward-Belle, G. (2017). Gender and intimate partner violence: The impact of patriarchal norms. *Journal of Family Violence*, 32(5), 455–466.

Higgins, G. (2024, September 28). Explicit 'deepfake' porn is on the rise - devastated victims include NZ teens. *1News*. <https://www.1news.co.nz/2024/09/28/explicit-deepfake-porn-is-on-the-rise-devastated-victims-include-nz-teens/>

Hindenburg Research. (2024, October). Roblox: Inflated key metrics for Wall Street and a pedophile hellscape for kids. Hindenburg Research. <https://hindenburesearch.com/roblox/>

Hinduja, S., & Patchin, J. W. (2024). Metaverse risks and harms among US youth: Experiences, gender differences, and prevention and response measures. *New Media & Society*, 0(0). <https://doi.org/10.1177/14614448241284413>

Hutchinson, A. (2023, October 15). X fined \$384K in Australia over failure to outline CSAM detection efforts. *Social Media Today*. <https://www.socialmediatoday.com/news/x-fined-384k-australia-over-failure-outline-csam-detection-efforts/696634/>

Independent Inquiry Child Sexual Abuse. (2023). J.5: The Online Safety Bill. The Report of the Independent Inquiry into Child Sexual Abuse. <https://www.iicsa.org.uk/reports-recommendations/publications/inquiry/final-report/ii-inquirys-conclusions-and-recommendations-change/part-j-evolving-challenges/j5-online-safety-bill.html>

Insoll, T., Smith, J., & Brown, K. (2024). Social media as a vector for child trafficking: A global analysis. *Child Protection Quarterly*, 12(3), 45–60.

Insoll, T., Soloveva, V., Díaz Bethencourt, E., Nieminen, N., Leivo, K., Ovaska, A., & Vaaranen-Valkonen, N. (2024). What drives online child sexual abuse offending? Understanding motivations, facilitators, situational factors, and barriers. 2KNOW project.

Insoll, T., Díaz Bethencourt, E., Ovaska, A., Lahtinen, H.-M., & Vaaranen-Valkonen, N. (2024). Knowledge to prevent online sexual violence against children: Insights from a survey of child sexual abuse material offenders. 2KNOW Project. <https://www.suojellaanlapsia.fi/en/post/2know-preliminary-findings-report>

International Centre for Missing and Exploited Children. (2017). Online grooming of children for sexual purposes: Model legislation & global review. https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf

Internet Watch Foundation. (2023). Annual report 2023: Trends in self-generated CSAM and online exploitation. <https://www.iwf.org.uk>

Internet Watch Foundation. (2023). IWF annual report 2023. <https://www.iwf.org.uk/annual-report-2023/>

Internet Watch Foundation. (2024, October 18). Public exposure to 'chilling' AI child sexual abuse images and videos increases [Press release]. <https://www.iwf.org.uk/news-media/news/public-exposure-to-chilling-ai-child-sexual-abuse-images-and-videos-increases/>

INTERPOL. (2024). Global report on dark web activities and CSAM distribution. <https://www.interpol.int>

James, N. (2024, April 22). Nearly 140 roles proposed to go at Customs and DIA. Radio New Zealand. <https://www.rnz.co.nz/news/national/514913/nearly-140-roles-proposed-to-go-at-customs-and-dia>

Jang, Y., & Ko, B. (2023). Online safety for children and youth under the 4Cs framework - A focus on digital policies in Australia, Canada, and the UK. *Children. Global Pediatric Health*. <https://doi.org/10.3390/children10081415>

Johnson, J. A. (2019, August 16). RESEARCH SUMMARY: The rise of the modern online pornography industry: Descriptions and implications [Video]. National Centre on Sexual Exploitation. <https://vimeo.com/270534983>

Johnson, M. (2023, October 3). Five things you need to know about the Online Safety Bill. Big Brother Watch. <https://bigbrotherwatch.org.uk/blog/five-things-you-need-to-know-about-the-online-safety-bill/>

Journal of Experimental Child Psychology. (2022). The effectiveness of spaced exposure for teaching online safety. *Journal of Experimental Child Psychology*, 122, 1–10.

Kaitai-Mullane, A. S. (2022). Decolonising Taara: Representations of wāhine Māori from early colonisation into contemporary pornography. University of Otago.

Kato, M. (2024). Advocacy for restricting child-like manga: Perspectives from a former offender. Protect Children Publishing.

Kato, T. (2022, October 4). He abused kids for 24 years. Now he wants manga sexualizing children to be banned. VICE World News. <https://www.vice.com/en/article/manga-abuse-children-japan-sexual>

Kilmeade, B. (2024, October 29). Tristian Harris warns parents of the potentially deadly consequences of AI chatbots manipulating our children [Radio broadcast]. Fox. <https://radio.foxnews.com/2024/10/29/tristian-harris-warns-parents-of-the-potentially-deadly-consequences-of-ai-chatbots-manipulating-our-children/>

Kira, B., & Mendes, L. (2023, November 13). A primer on the UK Online Safety Act: Key aspects of the new law and its road to implementation. Verfassungsblog. <https://verfassungsblog.de/a-primer-on-the-uk-online-safety-act/>

Kirklees Safeguarding Children. (2023). Domestic abuse strategy 2022–2027. <https://www.kirkleessafeguardingchildren.co.uk/wp-content/uploads/2023/08/Domestic-Abuse-Strategy-2022-2027-FINAL.pdf>

Korea Institute for Health and Social Affairs. (2020). Screen time and socioeconomic status among Korean youth. <https://www.kihasa.re.kr/>

Krahé B, Tomaszewska P, Schuster I. (2022). Links of perceived pornography realism with sexual aggression via sexual scripts, sexual behavior, and acceptance of sexual coercion: A study with German university students. *International Journal of Environmental Research and Public Health*, 19(1), 63. <https://doi.org/10.3390/ijerph19010063>

Lazimi, S. (2025). Beyond safety: Age assurance as a trust-building investment for online platforms. Yubo. <https://news.crunchbase.com/media-entertainment/startup-online-platform-safety-age-assurance-lazimi-yubo/>

Leask, A. (2024, November 24). TikTok shock: 'Scary' content pushed to social media feed set up for 13-year-old. NZ Herald. <https://www.nzherald.co.nz/nz/tiktok-shock-scary-content-pushed-to-social-media-feed-set-up-for-13-year-old/H7MAVPX53BBC7FS4XZ7Y2TXZWE/>

Lexology. (2024). Online safety and data protection developments. <https://www.lexology.com/library/detail.aspx?g=bc84de02-a88d-46dc-a33a-7bf1d4236a07>

Lim, M. S., Carrotte, E. R., & Hellard, M. E. (2016). The impact of pornography on gender-based violence, sexual health and well-being: what do we know?. *J Epidemiology Community Health*, 70(1), 3

Longpre, S., Mahari, R., Lee, A., Lund, C., Oderinwale, H., Brannon, W., Saxena, N., Obeng-Marnu, N., South, T., Hunter, C., Klyman, K., Klamm, C., Schoelkopf, H., Singh, N., Cherep, M., Anis, A., Dinh, A., Chitongo, C., Yin, D., Sileo, D., Mataciunas, D., Misra, D., Alghamdi, E., Shippole, E., Zhang, J., Materzynska, J., Qian, K., Tiwary, K., Miranda, L., Dey, M., Liang, M., Hamdy, M., Muennighoff, N., Ye, S., Kim, S., Mohanty, S., Gupta, V., Sharma, V., Minh Chien, V., Zhou, X., Li, Y., Xiong, C., Villa, L., Biderman, S., Li, H., Ippolito, D., Hooker, S., Kabbara, J., & Pentland, S. (2024). Consent in crisis: The rapid decline of the AI data commons. *arXiv*. <https://doi.org/10.48550/arXiv.2407.14933>

Louisiana Legislature. (2024). Senate Bill 175 (SB175). <https://legiscan.com/LA/text/SB175/id/2832119>

Lucy Faithfull Foundation. (n.d.). Faithfull paper: Chatbots. https://lff-spaces-cdn.lon1.digitaloceanspaces.com/lff-files/Faithfull_Paper_Chatbots.pdf

Lucy Faithfull Foundation. (n.d.). Project intercept: Revolutionising how we stop online child sexual abuse. <https://www.lucyfaithfull.org.uk/project-intercept-a-million-pound-investment-to-revolutionise-how-we-stop-online-child-sexual-abuse/>

Maas MK, Bray BC, Noll JG. Online sexual experiences predict subsequent sexual health and victimization outcomes among female adolescents: a latent class analysis. *J Youth Adolesc*. 2019;

Maas, M. K., Wright, P. J., Rothman, E. F., Nelson, K. M., Weigle, P., & Herbenick, D. (2025). Pornography use during adolescence: The current state of knowledge and recommendations. In D. A. Christakis & L. Hale (Eds.), *Handbook of children and screens*. Springer. https://doi.org/10.1007/978-3-031-69362-5_47

Makes Sense. (2024). Advocacy impact report: Search engine modifications for rape-related content. <https://www.makesense.org.nz>

Marchal, N., Xu, R., Elasmr, R., Gabriel, I., Goldberg, B., & Isaac, W. (2024). Generative AI misuse: A taxonomy of tactics and insights from real-world data [Preprint]. *arXiv*. <https://doi.org/10.48550/arXiv.2406.13843>

Marr, B. (2025, March 18). Sex and intimacy in the generative AI era. Bernard Marr. <https://bernardmarr.com/sex-and-intimacy-in-the-generative-ai-era/>

McKibbin, G., Humphreys, C., & Hamilton, B. (2017). "Talking about child sexual abuse would have helped me": Young people who sexually abused reflect on preventing harmful sexual behavior. *Child Abuse and Neglect*, 70, 210–221. <https://doi.org/10.1016/j.chiabu.2017.06.018>

Medierådet for Børn og Unge. (n.d.). Safer Internet Centre Denmark. <https://medieraadet.dk/sikker-internet-center-danmark/safer-internet-centre-denmark>

Microsoft. (2021). Microsoft submission to the Governance and Administration Select Committee.

Ministry of Business, Innovation and Employment. (2021, March 16). Plan of action against forced labour, people trafficking and slavery [Proactive release].

<https://www.mbie.govt.nz/dmsdocument/13607-plan-of-action-against-forced-labour-people-trafficking-and-slavery-proactiverelease-pdf>

Ministry of Education (New Zealand). (n.d.). Recommendations for the use of digital technologies: Schools, kura and early childhood education.

<https://web-assets.education.govt.nz/s3fs-public/2025-02/Recommendations-WIP13.pdf>

Ministry of Justice. (2020, August 27). Learn about the justice system. New Zealand Government. <https://www.justice.govt.nz/about/learn-about-the-justice-system/how-the-justice-system-works/>

Ministry of Justice. (2021). New Zealand Crime and Victims Survey: Māori victimisation in Aotearoa New Zealand. New Zealand Government.

<https://www.justice.govt.nz/assets/Maori-victimisation-report-v2.02-20220214-fin.pdf>

Ministry of Justice. (2022). New Zealand Crime and Victims Survey: Survey findings—Cycle 4 report descriptive statistics. New Zealand Government. <https://www.justice.govt.nz/justice-sector-policy/research-data/nzcvs>

Ministry of Justice. (2023). New Zealand Crime and Victims Survey Cycle 5 (2021/22) data tables. New Zealand Government. <https://www.justice.govt.nz/>

Ministry of Justice. (2023). Sexual offences data table. New Zealand Government. <https://www.justice.govt.nz/justice-sector-policy/research-data/justice-statistics/data-tables/>

Ministry of Social Development. (2002). Censorship in New Zealand: The policy challenges of new technology. Social Policy Journal, 19, 1–13.

<https://www.msd.govt.nz/about-msd-and-our-work/publications-resources/journals-and-magazines/social-policy-journal/spj19/censorship-new-zealand-challenges19-pages1-13.html>

Ministry of Social Development. (2021). Voices of adults who experienced sexual abuse in childhood: Findings from the qualitative research phase. New Zealand Government. <https://www.msd.govt.nz>

Ministry of Social Development. (2002). Te Rito: New Zealand Family Violence Prevention Strategy. New Zealand Government.

<https://www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/planning-strategy/te-rito/te-rito.pdf>

Ministry of Social Development. (2024, November). The Child and Youth Strategy 2024–2027. New Zealand Government.

<https://www.msd.govt.nz/documents/about-msd-and-our-work/child-youth-wellbeing/strategy-and-plan/the-child-and-youth-strategy-2024-27.pdf>

Ministry of Women. (2023). Preventing violence against women. New Zealand Government. <https://www.women.govt.nz/womens-safety/preventing-violence-against-women>

Mississippi Legislature. (2024). House Bill 1126 (HB1126). Walker Montgomery Protecting Children Online Act. <https://legiscan.com/MS/bill/HB1126/2024>

Monk, D. (2017). The role of empathy and relationship skills in preventing gender-based violence. Journal of Social Issues, 73(3), 504–522. <https://doi.org/10.1111/josi.12242>

Monk, D., & Bowen, E. (2020). The influence of family violence on adolescent behavior and gender norms. Psychology of Violence, 10(2), 156–165. <https://doi.org/10.1037/vio0000255>

Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. Child Abuse & Neglect, 143, 106255. <https://doi.org/10.1016/j.chiabu.2023.106255>

Morrah, M. (2024, August 28). Harmful content accessed on primary school iPads despite \$33m safety spend. New Zealand Herald.

<https://www.nzherald.co.nz/nz/harmful-content-accessed-on-primary-school-ipads-despite-33m-safety-spend/5YLP6VUMDJEPGE4SPAQKNL2IY/>

Morrongiello, B. A., & Lasenby, J. (2019). The role of repeated exposure in online safety education for children. *Developmental Psychology*, 55(8), 1678–1689. <https://doi.org/10.1037/dev0000745>

Morrongiello, B. A., Zdzieborski, D., & Stewart, J. (2019). Evaluating the effectiveness of a brief safety education intervention for children: Evidence from a randomized controlled trial. *Journal of School Health*, 89(10), 803–811. <https://doi.org/10.1111/josh.12812>

Mulligan, J. (2024, September 4). It's not Watergate, but it's a story. *I Ate Auckland* [Substack]. <https://jessemulligan.substack.com/p/its-not-watergate-but-its-a-story>

Namirial Focus. (2024). France strengthens online protection through identity checks for pornographic websites. <https://focus.namirial.com/en/pornographic-sites-identity-check-france/>

National Center for Missing and Exploited Children. (2023, December 7). Devastating blow to child protection: Meta expands encryption. <https://www.missingkids.org/blog/2023/devastating-blow-child-protection-meta-expands-encryption>

National Center for Missing & Exploited Children. (2024). NCMEC Releases New Sextortion Data.

<https://www.missingkids.org/blog/2024/ncmec-releases-new-sex-tortion-data>

National Institute of Justice. (n.d.). The impact of witnessing intimate partner violence on boys' future behavior. <https://nij.ojp.gov>

National Library of New Zealand. (2024). Introduction to the Child and Youth Wellbeing Strategy.

<https://ndhadeliver.natlib.govt.nz/webarchive/20240412190031/https://www.childyouthwellbeing.govt.nz/our-aspirations/context/introduction-child-and-youth-wellbeing-strategy>

National Office for Child Safety Australia. (n.d.). The national strategy at a glance. Australian Government. <https://www.childsafety.gov.au/what-we-do/national-strategy>

National Office for Child Safety Australia. (2021). National Strategy to Prevent and Respond to Child Sexual Abuse 2021–2030. Australian Government. <https://www.childsafety.gov.au/resources/national-strategy-prevent-and-respond-child-sexual-abuse-2021-2030>

National Office for Child Safety. (2021). Summary of the National Strategy to Prevent and Respond to Child Sexual Abuse 2021–2030 and its action plans. Australian Government. <https://www.childsafety.gov.au/resources/summary-national-strategy-prevent-and-respond-child-sexual-abuse-2021-2030-and-its-action-plans>

NCMEC. (2024). CyberTipline 2023 annual report. National Center for Missing & Exploited Children. <https://www.missingkids.org>

Netsafe. (n.d.). Reports and research. <https://netsafe.org.nz/our-work/reports-and-research#research-reports>

Netsafe. (n.d.). About the Harmful Digital Communications Act (2015). <https://netsafe.org.nz/our-work/helpline-services/the-harmful-digital-communications-act>

Netsafe. (2020). New Zealand children's experiences of online risks and their perceptions of harm.

<http://globalkidsonline.net/wp-content/uploads/2020/02/Ng%C4%81taiohimatihikooAotearoaNZchildrensexperiencesofonlinerisksandharm.pdf>

Netsafe. (2021). Teens & Screens 2024 Report. The State of the Online Nation. <https://cdn.sanity.io/files/8y8wsx0z/production/595922cb8772a45974bf3dbf451c0cbe5f9d04ba.pdf>

Netsafe. (2023, August 17). Netsafe response to the Safer Online Services and Media Platforms consultation. <https://cdn.sanity.io/files/8y8wsx0z/production/37eac4f0c87bd621a1b85847e8f47b0e030784e3.pdf>

Netsafe. (2023). Annual report 2022/2023. <https://cdn.sanity.io/files/8y8wsx0z/production/4e16aba365bc064a3fe39f2f64ea4baa04aa4734.pdf>

Netsafe. (2024). Southern boost for online safety with new Netsafe office [Press release]. <https://www.scoop.co.nz/stories/SC2408/S00045/southern-boost-for-online-safety-with-new-netsafe-office.htm>

Netsafe. (2024). Understanding and combating child sexual abuse material (CSAM). <https://netsafe.org.nz/online-abuse-and-harassment/child-sexual-abuse-material-csam>

New Zealand Family Violence Clearinghouse. (2017). Child sexual abuse. <https://nzfvc.org.nz/our-work/data-summaries/child-sexual-abuse>

New Zealand Family Violence Clearinghouse. (2024, June 7). Budget 2024: Overview from the NZFVC. <https://nzfvc.org.nz/news/budget-2024-overview-nzfvc>

New Zealand Customs Service. (2024, April 23). NZ agencies urge young people to be safe online as reports of online child exploitation continue to rise. <https://www.customs.govt.nz/about-us/news/media-releases/nz-agencies-urge-young-people-to-be-safe-online-as-reports-of-online-child-exploitation-continue-to-rise/>

New Zealand Government. (n.d.). Guiding star sets new path for the elimination of family violence and sexual violence. New Zealand Government. <https://www.beehive.govt.nz/release/guiding-star-sets-new-path-elimination-family-violence-and-sexual-violence>

New Zealand Government. (2021). Govt acts to protect New Zealanders from harmful content. New Zealand Government. <https://www.beehive.govt.nz/release/govt-acts-protect-nzers-harmful-content>

New Zealand Government. (2024, June 18). Improvements to stopping digital child exploitation. New Zealand Government. <https://www.beehive.govt.nz/release/improvements-stopping-digital-child-exploitation>

New Zealand National Party. (2024). Social Media (Age-Restricted Users) Bill. <https://assets.national.org.nz/SocialMediaAge-RestrictedUsersBill.pdf>

New Zealand Police. (2024, April 23). NZ agencies urge young people to be safe online as reports of online child exploitation continue to rise [Press release]. <https://www.police.govt.nz/news/release/nz-agencies-urge-young-people-be-safe-online-reports-online-child-exploitation-continue>

OECD. (n.d.). Online safety and wellbeing. <https://www.oecd.org/en/topics/online-safety-and-well-being.html>

OECD. (2024). Towards digital safety by design for children. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital-safety-by-design-for-children_f1c86498/c167b650-en.pdf

Ofcom. (2020). Children and parents: Media use and attitudes report 2020. <https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2021>

Ofcom. (2024, February 8). Tackling child sexual abuse under the online safety regime. <https://www.ofcom.org.uk/online-safety/protecting-children/tackling-child-sexual-abuse-under-the-online-safety-regime/>

Ofcom. (2024, November 28). Online Nation 2024 report. https://www.ofcom.org.uk/__data/assets/pdf_file/0025/279123/online-nation-2024-report.pdf

Ofcom. (n.d.). Enforcing the Online Safety Act: Scrutinising illegal harms risk assessments. <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/enforcing-the-online-safety-act-scrutinising-illegal-harms-risk-assessments/>

Office of Juvenile Justice and Delinquency Prevention. (n.d.). Internet Crimes Against Children Task Force Program. <https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program>

Office of the Parliamentary Budget Officer. (2024, July 4). Bill C-63 (44-1): Establishment of a Digital Safety Commission, Ombudsperson, and Office [Legislative Costing Note]. <https://www.pbo-dpb.ca/en/publications/LEG-2425-008-M-online-harms-act-establishment-digital-safety-commission-ombudsperson-office-loi-prejudices-ligne-etablissement-commission-ombudsman-bureau-securite-numerique>

Office of the United Nations High Commissioner for Human Rights. (2024). UN expert alarmed by new emerging exploitative practices in online child sexual abuse. <https://www.ohchr.org/en/press-releases/2024/02/un-expert-alarmed-new-emerging-exploitative-practices-online-child-sexual>

OpenParliament.ca. (n.d.). Bill S-210: Status updates. <https://openparliament.ca/bills/44-1/S-210/>

Organisation for Economic Co-operation and Development (OECD). (2024). Towards digital safety by design for children (OECD Digital Economy Papers No. 363). OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital-safety-by-design-for-children_f1c86498/c167b650-en.pdf

Papp, L. J., Ward, L. M., & Marshall, R. A. (2022). Contributions of reality TV consumption to college women's endorsement of the heterosexual script and acceptance of sexualized aggression. *Psychology of Popular Media*, 11(4), 389–398. <https://doi.org/10.1037/ppm0000377>

Parliament of Australia. (n.d.). Infosheet 22 - Political parties. Australian Government. https://www.aph.gov.au/About_Parliament/House_of_Representatives/Powers_practice_and_procedure/00_-_Infosheets/Infosheet_22_-_Political_parties

Parliament of Australia. (2021). Online Safety Bill 2021. Australian Government. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/

Parliament of Australia. (2024–2025). Digital platforms milestones. Australian Government. https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/Chronologies/2024-25/Digital_Platforms_Milestones

Pataranutaporn, P., & Mahari, R. (2024, August). We need to prepare for 'addictive intelligence'. MIT Media Lab. <https://www.media.mit.edu/articles/we-need-to-prepare-for-addictive-intelligence/>

Patel, P. (2021). Foreword to Tackling child sexual abuse strategy. UK Home Office. <https://www.gov.uk/government/publications/tackling-child-sexual-abuse-strategy/tackling-child-sexual-abuse-strategy-accessible-version>

Pathmendra P, et al (2023). Exposure to Pornography and Adolescent Sexual Behavior: Systematic Review. *J Med Internet Res*.

Paulus, M. P., Squeglia, L. M., Bagot, K., Jacobus, J., Kuplicki, R., Breslin, F. J., ... & Tapert, S. F. (2019). Screen media activity and brain structure in youth: Evidence from the Adolescent Brain Cognitive Development (ABCD) study. *NeuroImage*, 185, 140–153. <https://doi.org/10.1016/j.neuroimage.2018.10.040>

Pereira, C. M., & Matos, P. M. (2021). Parenting styles and parental mediation of internet use: A study with adolescents and their parents. *Journal of Adolescence*, 88, 1–10. <https://doi.org/10.1016/j.adolescence.2021.01.006>

ParentsTogether Action. (2021, March 9). New study: One year into the pandemic, 82% of parents are concerned about their kids' screen time. <https://parentstogetheraction.org/new-study-one-year-into-the-pandemic-82-of-parents-are-concerned-about-their-kids-screen-time/>

Perrigo, B. (2018, August 20). The U.K. is about to regulate online porn, and free speech advocates are terrified. *TIME*. <https://time.com/5352875/uk-porn-block-age-verification/>

Peter, J., & Valkenburg, P. M. (2009). Adolescents' exposure to sexually explicit internet material and notions of women as sex objects: Assessing causality and underlying processes. *Journal of Communication*, 59(3), 407–433. <https://doi.org/10.1111/j.1460-2466.2009.01422.x>

Pettifer, S., Barrett, E., Marsh, J., Hill, K., Turner, P., & Flynn, S. (2020). The future of eXtended reality technologies, and implications for online child sexual exploitation and abuse. The University of Manchester.

Pew Research Center. (2021). Mobile technology and home broadband 2021. <https://www.pewresearch.org/internet/2021/06/03/mobile-technology-and-home-broadband-2021/>

Pew Research Center. (2023). How U.S. Mothers, Fathers Differ on Parenting. <https://www.pewresearch.org/social-trends/2023/01/24/gender-and-parenting/>

Pew Research Center. (2024). Parenting in America today. <https://www.pewresearch.org/social-trends/2023/01/24/parenting-in-america-today/>

PHCC. (n.d.). Social media and youth wellbeing: A need for a multi-layered public health approach.<https://www.phcc.org.nz/briefing/social-media-and-youth-wellbeing-need-multi-layered-public-health-approach>

Politico. (n.d.). France doubles down on social media age limit at 15. <https://www.politico.eu/article/france-doubles-down-on-social-media-age-limit-at-15/>

Prevent Together. (n.d.). Prevent Together initiative. <https://preventtogether.org>

Prevent Together. (2025). National plan to prevent child sexual abuse and exploitation. https://preventtogether.org/wp-content/uploads/2025/03/National-Plan_Jan2025.pdf

Protect Children. (2024). Tech platforms used by online child sexual abuse offenders.<https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse>

Protect Children. (2024). Victim contact trends in online child sexual exploitation. Protect Children. <https://www.protectchildren.fi>

Public Safety Canada. (2022, May 24). Summary of the evaluation of the expansion of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2022-vltn-nspcs-xpltn-smry/index-en.aspx>

Public Safety Canada. (2022, May 24). Summary of the evaluation of the expansion of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2022-vltn-nspcs-xpltn/index-en.aspx#b03>

Public Safety Canada. (2023). Actions to combat online child sexual exploitation.<https://www.publicsafety.gc.ca/cnt/cntrng-crm/chld-sxl-xpltn-ntmnt/actns-nln-chld-sxl-xpltn-en.aspx>

Public Safety Canada. (2025, March 20). Government of Canada invests in protecting children and youth from online sexual exploitation [Press release]. <https://www.canada.ca/en/public-safety-canada/news/2025/03/government-of-canada-invests-in-protecting-children-and-youth-from-online-sexual-exploitation.html>

Radesky, J. S., Schumacher, J., & Zuckerman, B. (2015). Mobile and interactive media use by young children: The good, the bad, and the unknown. *Pediatrics*, 135(1), 1–3. <https://doi.org/10.1542/peds.2014-2251>

Radio New Zealand. (2024, April 23). Increase in reports of online child exploitation.<https://www.rnz.co.nz/news/national/514970/increase-in-reports-of-online-child-exploitation>

Radio New Zealand. (2024, June 19). Internal Affairs job cuts will lead to more Kiwis being scammed online, union says. <https://www.rnz.co.nz/news/national/519992/internal-affairs-job-cuts-will-lead-to-more-kiwis-being-scammed-online-union-says>

Radio New Zealand. (2024, September 10). Tauranga man sentenced for possessing extreme material depicting sexual exploitation of children. <https://www.rnz.co.nz/news/national/527598/tauranga-man-sentenced-for-possessing-extreme-material-depicting-sexual-exploitation-of-children>

Reset. (2024, February). Accountability, the Online Safety Act, and the Basic Online Safety Expectations: Can safety standards be enforceable? [Policy Briefing]. <https://au.reset.tech/uploads/Accountability-&-Safety-requirements-0424-V2.pdf>

- Rideout, V., & Robb, M. B. (2021). The Common Sense Census: Media use by tweens and teens, 2021. Common Sense Media.
<https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021>
- Rideout, V., Robb, M. B., & Spicer, P. (2022). The Common Sense Census: Media use by kids age zero to eight, 2022. Common Sense Media.
<https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-kids-age-zero-to-eight-2020>
- Robb, M.B., & Mann, S. (2023). Teens and pornography. San Francisco, CA: Common Sense Media.
- Rodenhizer, K. A. E., & Edwards, K. M. (2019). The impacts of sexual media exposure on adolescent and emerging adults' dating and sexual violence attitudes and behaviours: A critical review of the literature. *Trauma, Violence, & Abuse*, 20(4), 439–452. <https://doi.org/10.1177/1524838017717744>
- ROOST. (2025, February). Christchurch Call partners with ROOST for open-source AI tools to tackle TVEC. <https://roost.tools/>
- Rose, R. (1991). What is lesson drawing? *Journal of Public Policy*, 11(1), 3–30. <https://doi.org/10.1017/S0143814X00004918>
- Rosenthal, H. E., Mehta, S., Behnam, R., Lin, A., Hatef, C., Chow, N., O'Connor, M., & Milanaik, R. (2022). Teen Tinder? An analysis of app-store reviews of adolescent “friendship” apps. *Pediatrics*, 149(1), 11.
<https://publications.aap.org/pediatrics/article/149/1%20Meeting%20Abstracts%20February%202022/11/185704/Teen-Tinder-An-Analysis-of-App-store-Reviews-of>
- Safeguarding Children United Kingdom. (n.d.). Child exploitation. <https://www.safeguardingchildren.co.uk/parents-carers/child-exploitation/>
- Salter, M., & Sokolov, S. (2023). “Talk to strangers!” Omegle and the political economy of technology-facilitated child sexual exploitation. *Journal of Criminology*, 57(2), 121–137. <https://doi.org/10.1177/26338076231194451>
- Salter, M., Woodlock, D., & Wong, T. (2024). The sexual politics of technology industry responses to online child sexual exploitation during COVID-19: “This pernicious elitism.” *Child Abuse & Neglect*.
<https://www.academia.edu/109181588>
- Sandvik, M., Nasset, M. B., Berg, A., & Søndena, E. (2017). The Voices of young sexual offenders in Norway: A qualitative study. *Open Journal of Social Sciences*
- Save the Children & Netsafe. (April 10, 2025). Children speak out: What tamariki and rangatahi really want from a safer internet [Press release].
<https://www.savethechildren.org.nz/media-hub/what-tamariki-really-want-from-a-safer-internet>
- Schittenhelm, C., Kops, M., Moosburner, M. et al. Cybergrooming Victimization Among Young People: A Systematic Review of Prevalence Rates, Risk Factors, and Outcomes. *Adolescent Research Review*. (2024).
<https://doi.org/10.1007/s40894-024-00248-w>
- SchoolTV. (2024). Special report: Navigating AI relationships. https://schooltv.me/wellbeing_news/special-report-navigating-ai-relationships-au
- Security Hero. (2023). 2023 state of deepfakes. <https://www.securityhero.io/state-of-deepfakes/>
- SEMrush. (n.d.). Adult porn sites in New Zealand. SEMrush. Retrieved March 5, 2025, from <https://www.semrush.com/>
- Setty, E., & Dines, G. (2024). Why media literacy education must include pornography literacy: A call to action. *Sex Education*, 24(2), 234–248.

- Shepherd, H. J., & Byrne, S. (2023). Children's exposure to harmful online content and parental mediation strategies: A systematic review. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 17(4), Article 2. <https://doi.org/10.5817/CP2023-4-2>
- Shor, E., & Seida, K. (2019). "Harder and harder"? Is mainstream pornography becoming increasingly violent and do viewers prefer violent content? *The Journal of Sex Research*, 56(1), 16-28.
- Siddique, H. (2024, May 27). More than 300m children victims of online sexual abuse every year. *The Guardian*. <https://www.theguardian.com/society/article/2024/may/27/more-than-300m-children-victims-of-online-sexual-abuse-every-year>
- SimilarWeb. (n.d). Adult porn sites in New Zealand. <https://www.similarweb.com/>
- Simpson Grierson. (2023, July 13). Safer online services and media in New Zealand - Proposals for change. <https://www.simpsongrierson.com/insights-news/legal-updates/safer-online-services-and-media-in-new-zealand-proposals-for-change>
- Sing, F., & Lyons, A. (2024, June 24). Big tech companies were open to online safety regulation—why did NZ's government scrap the idea? *The Conversation*. <https://theconversation.com/big-tech-companies-were-open-to-online-safety-regulation-why-did-nzs-government-scrap-the-idea-232371>
- Smahel, D., & Smahelova, M. (2022). Children's engagement with risky content online: A longitudinal study. *Media and Communication*, 10(3), 116–129.
- Smahel, D., MacHackova, H., & Machackova, S. (2023). EU Kids Online 2023: Children's online experiences across Europe. London School of Economics. <https://www.eukidsonline.net>
- Smith, L. W., Liu, B., Degenhardt, L., Richters, J., Patton, G., Wand, H., ... & Guy, R. (2016). Is sexual content in new media linked to sexual risk behaviour in young people? A systematic review and meta-analysis. *Sexual Health*, 13(6), 501-515.
- Staksrud, E., Livingstone, S., & Haddon, L. (2020). What do we know about children's use of online pornography? *Information, Communication & Society*, 23(2), 276–291. <https://doi.org/10.1080/1369118X.2018.1479342>
- Statista. (n.d.). Steam. Retrieved July 12, 2024, from <https://www.statista.com/topics/4282/steam/#editorsPicks>
- Statista. (n.d.). OnlyFans: Global monthly visits 2021–2023. <https://www.statista.com/statistics/1291891/onlyfans-global-monthly-visits/>
- Statista (2015). PMC, Parental Perception of Children's Online Behaviour (Australian study)
- Stevens Aubrey, J., Gahler, H., Daniels, E. A., Choi, H. J., & Speno, A. G. (2024). Examining relations between sexualizing media exposure and sexting attitudes and behaviors among U.S. adolescents. *Archives of Sexual Behavior*, 53(10), 4065–4078. <https://link.springer.com/article/10.1007/s10508-024-02984-5?fromPaywallRec=true>
- Stop It Now. (n.d.). Preventing child sexual abuse. <https://www.stopitnow.org.uk/>
- Substance Abuse and Mental Health Services Administration. (2022). SAMHSA's concept of trauma and guidance for a trauma-informed approach (HHS Publication No. PEP22-06-01-005). U.S. Department of Health and Human Services. <https://www.samhsa.gov>
- Sun, C., Bridges, A. J., Johnson, J. A., & Ezzell, M. B. (2016). Pornography and the male sexual script: An analysis of consumption and sexual relations. *Archives of Sexual Behavior*, 45(4), 983–994. <https://doi.org/10.1007/s10508-014-0391-2>

Tasmanian Policy Exchange. (2024). A comparative review of strategies to prevent and respond to child sexual abuse. University of Tasmania.

https://keepingchildrensafe.tas.gov.au/documents/29/FINAL_-_UTAS_-_A_comparative_review_of_strategies_to_prevent_and_respond_to_ch_RzHpkXr.pdf

Taylor, J. (2023, August 19). Australia eyes UK online bill in fight with tech companies over encryption and child safety. The Guardian.

<https://www.theguardian.com/australia-news/2023/aug/20/australia-eyes-uk-online-bill-in-fight-with-tech-companies-over-encryption-child-safety>

Taylor, J. (2023, September 6). AFP calls on public to donate childhood photos in bid to combat child abuse with AI. The Guardian.

<https://www.theguardian.com/australia-news/2023/sep/06/afp-calls-on-public-to-donate-childhood-photos-in-bid-to-combat-child-abuse-with-ai>

Taylor, J. (2024, May 1). Australia's online safety regulator has drawn a line in the sand for X. Will she prevail? The Guardian.

<https://www.theguardian.com/australia-news/2024/may/02/australias-online-safety-regulator-has-drawn-a-line-in-the-sand-for-x-will-she-prevail>

Tech Coalition. (2023, November). Announcing Lantern: The first child safety cross-platform signal sharing program. <https://www.technologycoalition.org/newsroom/announcing-lantern>

Tei, S., Fujino, J., & Murai, T. (2025). Navigating the self online. *Frontiers in Psychology*, 16, Article 1499039. <https://doi.org/10.3389/fpsyg.2025.1499039>

Tennessee General Assembly. (2024). House Bill 2163 (HB2163). <https://wapp.capitol.tn.gov/apps/Billinfo/default.aspx?BillNumber=HB2163&ga=113>

Te Puna Aonui. (2023). Outcomes and measurement framework. New Zealand Government. <https://tepunaaonui.govt.nz/assets/Uploads/Outcomes-and-Measurement-Framework.pdf>

Te Puna Aonui. (2023). Responding, healing, strengthening: Questions from participants in the Annual Te Aorerekura Hui 2023. New Zealand Government.

https://tepunaaonui.govt.nz/assets/Uploads/Hui-Questions-and-Answers-FINAL_.pdf

Te Puna Aonui. (2023, September). Te Aorerekura: The National Strategy to Eliminate Family Violence and Sexual Violence Outcomes and Measurement Framework. New Zealand Government.

<https://tepunaaonui.govt.nz/assets/Uploads/Outcomes-and-Measurement-Framework.pdf>

Te Puni Kōkiri. (2015). Understanding whānau-centred approaches. <https://www.tpk.govt.nz/documents/download/1025/understanding-whanau-centred-approaches.pdf>

Te Rōpū Tautoko. (2021). Listening to survivors: Experiences and impacts of sexual abuse in faith-based settings. <https://tautoko.catholic.org.nz>

The Behavioural Architects (Upton, J., Hazell, A., Abbott, R., & Pilling, K.). (2020). The relationship between pornography use and harmful sexual attitudes and behaviours: A literature review. Government Equalities Office.

The Code. (n.d.). Home. <https://thecode.org.nz>

The Jerusalem Post. (2024). Science around the world. <https://www.jpost.com/science/science-around-the-world/article-851782>

The Law Association of New Zealand. (2023). Government proposes content regulator. <https://thelawassociation.nz/govt-proposes-content-regulator/>

The University of Manchester. (2020). The future of eXtended reality technologies, and implications for online child sexual exploitation and abuse. <https://documents.manchester.ac.uk/display.aspx?DocID=62042>

Third, A., Kennedy, Ú., Lala, G., Rajan, P., Sardarabady, S., & Tatam, L. (2024). Protecting children from online grooming: Cross-cultural, qualitative and child-centred data to guide grooming prevention and response. https://resourcecentre.savethechildren.net/pdf/REPORT_PROTECTING-CHILDREN_FINAL.pdf

Thompson, E., & Lamphere-Englund, G. (2024, November). 30 years of trends in terrorist and extremist games. Global Network on Extremism and Technology (GNET). <https://gnet-research.org/2024/11/01/30-years-of-trends-in-terrorist-and-extremist-games/>

Thompson, K., & Haninger, K. (2024). Hentai and the pornification of childhood: How the porn industry just made the case for regulation. DigitalCommons@URI. <https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1048&context=jmle>

Thorburn, Brandee & Gavey, Nicola & Single, Grace & Wech, April & Calder-Dawe, Octavia & Benton-Greig, Paulette. (2021). To send or not to send nudes: New Zealand girls critically discuss the contradictory gendered pressures of teenage sexting. Women's Studies International Forum.

Thorn. (2024). Youth perspectives on online safety, 2023. <https://www.thorn.org/research/library/2023-youth-perspectives-on-online-safety/>

Thorn. (2023, November). Youth perspectives on online safety, 2022: An annual report of youth attitudes and experiences. Thorn. https://info.thorn.org/hubfs/Research/22_YouthMonitoring_Report.pdf

Thorn, & BSG. (2024). Youth perspectives on online safety, 2023: An annual report of youth attitudes and experiences. https://info.thorn.org/hubfs/Research/Thorn_23_YouthMonitoring_Report.pdf

Thorn. (2024). Emerging threats: Nudify apps and their impact on youth. <https://www.thorn.org>

Thorn. (2024, August 14). Youth perspectives on online safety, 2023. <https://www.thorn.org/research/library/2023-youth-perspectives-on-online-safety/>

Thorn and WeProtect Global Alliance. (2024). Evolving Technologies Horizon Scan: A review of technologies carrying notable risk and opportunity in the fight against technology-facilitated child sexual exploitation

TikTok Australia. (n.d.). Submission regarding the online safety age-restricted social media platforms rules. TikTok Newsroom. <https://newsroom.tiktok.com/en-au/tiktok-australias-submission-regarding-the-online-safety-age-restricted-social-media-platforms-rules>

Tokunaga, R. S., Wright, P. J., & Roskos, J. E. (2019). Pornography and impersonal sex. Human Communication Research, 45(1), 78–118. <https://doi.org/10.1093/hcr/hqy014>

Tomaszewska, P., & Krahé, B. (2018). Predictors of sexual aggression victimization and perpetration among Polish university students: A longitudinal study. Archives of Sexual Behavior, 47(2), 493–505. <https://doi.org/10.1007/s10508-016-0823-2>

Trengove, M., Kazim, E., Almeida, D., Hilliard, A., Zannone, S., & Lomas, E. (2022). A critical review of the Online Safety Bill. Patterns, 3(10), 100544. <https://doi.org/10.1016/j.patter.2022.100544>

TRG. (2024). Wave 3 research findings: Digital well-being index. <https://values.snap.com/safety/>

UBS Chief Investment Office. (2024, June 10). Artificial intelligence: Sizing and seizing the investment opportunity. UBS Group AG.

UK Home Office. (2021). Tackling child sexual abuse strategy. <https://www.gov.uk/government/publications/tackling-child-sexual-abuse-strategy>

UNICEF. (n.d.). What is the UN Convention on the Rights of the Child? <https://www.unicef.org.uk/what-we-do/un-convention-child-rights/>

UNICEF. (2014, September). Ending violence against children: Six strategies. Child Protection Unit. <https://www.unicef.org/media/66906/file/Ending-Violence-Against-Children-Six-strategies-For-Action.pdf>

UNICEF. (2022). The digital age and children's rights: Balancing safety and participation. <https://www.unicef.org>

UNICEF. (2023). Framing the future: How to deliver on digital experiences for children. <https://www.unicef.org/media/121071/file/Framing%20the%20Future%20.pdf>

UNICEF Innocenti - Global Office of Research and Foresight. (2023). The role of social media in facilitating online child sexual exploitation and abuse (Disrupting Harm Data Insight 7). Safe Online.

United Kingdom Government. (2020). Interim code of practice: Child online safety. Home Office.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944034/1704___HO___INTERIM_CODE_OF_PRACTICE_CSEA_v.2.1_14-12-2020.pdf

United Kingdom Government. (2021). Guidance: Protecting children from online sexual exploitation and abuse. <https://www.gov.uk/guidance/child-online-safety-protecting-children-from-online-sexual-exploitation-and-abuse>

United Kingdom Government. (2021, June 7). Policy paper: Tackling child sexual abuse strategy (accessible version).

<https://www.gov.uk/government/publications/tackling-child-sexual-abuse-strategy/tackling-child-sexual-abuse-strategy-accessible-version#executive-summary>

United Kingdom Government. (2022, January 31). Online Safety Bill impact assessment. https://assets.publishing.service.gov.uk/media/6231dc9be90e070ed8233a60/Online_Safety_Bill_impact_assessment.pdf

United Kingdom Government. (2023). Tackling child sexual abuse strategy. <https://www.gov.uk/government/publications/tackling-child-sexual-abuse-strategy/tackling-child-sexual-abuse-strategy-accessible-version>

United Kingdom Government. (2023, October 26). Online safety. Home Office. <https://www.gov.uk/government/news/uk-children-and-adults-to-be-safer-online-as-world-leading-bill-becomes-law>

United Kingdom Government. (2024). UK children and adults to be safer online as world-leading bill becomes law.

<https://www.gov.uk/government/news/uk-children-and-adults-to-be-safer-online-as-world-leading-bill-becomes-law>

United Kingdom Government. (2024). UK-US statement on the protection of children online. Department for Science, Innovation and Technology.

<https://www.gov.uk/government/publications/uk-us-statement-on-the-protection-of-children-online/uk-us-statement-on-the-protection-of-children-online>

United Kingdom Government. (2024, February 21). Tougher laws to protect children from sexual abuse. Home Office. <https://www.gov.uk/government/news/tougher-laws-to-protect-children-from-sexual-abuse>

United Nations Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25).

<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

United Nations Office on Drugs and Crime. (2023). Global report on trafficking in persons: Focus on children. <https://www.unodc.org>

U.S. Department of Homeland Security. (2024, April 30). DHS completes Secretary's commitment to a peer-to-peer exchange with the Government of Australia as part of the Australia-United States Joint Council on Combating Online Child Sexual Exploitation. <https://www.dhs.gov/news/2024/04/30/dhs-completes-secretarys-commitment-peer-peer-exchange-government-australia-part>

van der Kolk, B. A., & Post, R. M. (2020). The neurobiology of trauma: Pathways to recovery. *Journal of Traumatic Stress*, 33(5), 671–680. <https://doi.org/10.1002/jts.22565>

Vera-Gray, F., McGlynn, C. M. S., Kureshi, I., & Butterby, K. (2021). Sexual violence as a sexual script in mainstream online pornography. British Journal of Criminology. <https://ssrn.com/abstract=4380281>

VerifyMy. (2024, February 6). Young people encounter harmful, age-restricted and illegal content within minutes of going online.
<https://verifymy.io/blog/young-people-encounter-harmful-age-restricted-and-illegal-content-within-minutes-of-going-online/>

Vincent, J. (2024, May 16). Reddit blocks OpenAI's ChatGPT from accessing its data in API dispute. The Verge. <https://www.theverge.com/2024/5/16/24158529/reddit-openai-chatgpt-api-access-advertising>

Visual Capitalist. (2023, January 24). Visual Capitalist. <https://www.visualcapitalist.com>

Waterman, Emily A., Rose Wesche, Grace Morris, Katie M. Edwards, and Victoria L. Banyard. (2022). 'Prospective Associations Between Pornography Viewing and Sexual Aggression Among Adolescents'. Journal of Research on Adolescence.

WBur. (2024, October). Roblox attempts to bar child predators as short sellers target the popular game platform. <https://www.wbur.org/hereandnow/2024/10/21/roblox-child-predators-safety>

Weam. (2024, January 29). Character.AI statistics you need to know in 2024. <https://weam.ai/blog/guide/character-ai/character-ai-statistics/>

Weekes, J. (2024, February 2). Online bullying and cyber abuse: Dramatic increase in stalking and harassment. New Zealand Herald.
<https://www.nzherald.co.nz/business/online-bullying-cyber-abuse-dramatic-increase-in-stalking-harassment-netsafe-asks-new-govt-ministers-for-help/3QSVTQ2LWZEURI2ZJGBDN4QFU4/>

Wellington City Council. (n.d.). Sexual violence prevention roadmap.
<https://wellington.govt.nz/-/media/community-support-and-resources/community-safety/files/sexual-violence-prevention/sexual-violence-prevention-roadmap.pdf>

WeProtect Global Alliance. (2022). Framing the future: How the Model National Response framework is supporting national efforts to end child sexual exploitation and abuse online.
<https://www.weprotect.org/resources/frameworks/model-national-response/>

WeProtect Global Alliance. (2023). Globally aligned legislation to protect children online.<https://www.weprotect.org/global-threat-assessment-23/globally-aligned-legislation/>

WeProtect Global Alliance. (2023). Global threat assessment 2023: Online child sexual exploitation and abuse. WeProtect Global Alliance.
<https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf>

WeProtect Global Alliance. (2023). Global threat assessment: Alarming escalation in child sexual abuse online revealed by Global Threat Assessment 2023 [Press Release].
<https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-Press-Release.pdf>

WeProtect Global Alliance. (2024, April). Policy briefing: UK Online Safety Act. Co-funded by the European Union. <https://www.weprotect.org/wp-content/uploads/UK-Online-Safety-Act-Policy-Briefing.pdf>

Whyte, A. (2024, April 16). Digital safety and anti-money laundering jobs face axe in Internal Affairs proposal. The Post. <https://www.thepost.co.nz/politics/350253534/digital-safety-anti-money-laundering-jobs-cut-proposal>

Wikipedia contributors. (2024, October 9). Commonwealth realm. Wikipedia. https://en.wikipedia.org/w/index.php?title=Commonwealth_realm&oldid=1250293559

Wilde, T. (2021, April 28). Most game devs don't think Steam earns its 30% revenue cut. PC Gamer. <https://www.pcgamer.com/most-game-devs-dont-think-steam-earns-its-30-revenue-cut/>

Wodecki, B. (2023, February, 4). ChatGPT may be the fastest growing app of all time. AI Business. <https://aibusiness.com/nlp/ubs-chatgpt-is-the-fastest-growing-app-of-all-time>

Wolbers, Heather & Dowling, Christopher. (2024). Routine online activities and vulnerability to dating app facilitated sexual violence. <https://www.aic.gov.au/publications/tandi/tandi704>

Wolbers H, Cubitt T, Napier S, Cahill M, Nicholas M, Burton M & Giunta K (2025). Sexual extortion of Australian adolescents: Results from a national survey. Trends & issues in crime and criminal justice no. 712. Canberra: Australian Institute of Criminology. <https://doi.org/10.52922/ti77819>

World Economic Forum. (2025, April). 'Adolescence' has sparked a digital safety debate: A new report offers a fresh approach to tackling online harm
<https://www.weforum.org/stories/2025/04/adolescence-digital-safety-online-harm>

World Economic Forum. (2025, March). The intervention journey: A roadmap to effective digital safety measures.
https://reports.weforum.org/docs/WEF_The_Intervention_Journey_A_Roadmap_to_Effective_Digital_Safety_Measures_2025.pdf

Wright, P. J. (2011). Mass media effects on youth sexual behavior assessing the claim for causality. Annals of the International Communication Association, 35(1), 343–385.
<https://doi.org/10.1080/23808985.2011.11679121>

Wright, M. F., & Wachs, S. (2021). Adolescents' psychological distress and associations with cybervictimization and parental mediation. Computers in Human Behavior, 119, 106715.
<https://doi.org/10.1016/j.chb.2021.106715>

Wright, P. J., Tokunaga, R. S., & Kraus, A. (2016). A meta-analysis of pornography consumption and actual acts of sexual aggression in general population studies. Journal of Communication, 66(1), 183-205.
<https://doi.org/10.1111/jcom.12201>

Wurtele, S. K., & Kenny, M. C. (2010). Partnering with parents to prevent childhood sexual abuse. Child Abuse & Neglect, 34(11), 867–872.
https://www.researchgate.net/publication/229459918_Partnering_with_Parents_to_Prevent_Childhood_Sexual_Abuse

Ybarra, M. L., Mitchell, K. J., Hamburger, M., Diener-West, M., & Leaf, P. J. (2011). X-rated material and perpetration of sexually aggressive behavior among children and adolescents: Is there a link?. Aggressive Behavior, 37(1), 1-18.

Ybarra, M. L., & Thompson, R. E. (2018). Predicting the emergence of sexual violence in adolescence. Prevention Science, 19(4), 403-415.

Yen, A. (2023). The Online Safety Act doesn't protect encryption, but Ofcom can. Proton. <https://proton.me/blog/online-safety-act>

Zhao, W., Ren, X., Hessel, J., Cardie, C., Choi, Y., & Deng, Y. (2024). WILDCHAT: 1M chatGPT interaction logs in the wild. arXiv. <https://arxiv.org/pdf/2405.01470v1>

Zander, N. (2021) Contrary Research. Character.ai. Contrary. <https://research.contrary.com/company/character-ai>

Zurcher, A. (2023, September 27). Meta accused of facilitating child sexual abuse. BBC News. <https://www.bbc.com/news>

Co-authors:

Holly Brooker, Makes Sense
Rory Birkbeck, Safe Surfer
Jo Robertson, Makes Sense

Contributing author:

Nikki Denholm, The Light Project.

Disclaimer

The information in The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand Report is intended to provide an overview of digital sexual harms and recommendations to keep young people safe online. All reasonable measures have been taken to ensure the quality and accuracy of the information published. However ACC makes no warranty, express or implied, nor assumes any legal liability or responsibility for the accuracy, suitability, correctness, completeness or use of any information in The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand Report. Nothing contained in The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand Report is, or shall be relied on as a promise or representation by ACC on any of the matters considered in The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand Report. Information contained in The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand Report is current as at the date of the Report, and may not reflect any event or circumstances which occur after the date of the Report. The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand Report does not necessarily represent the official view of ACC or represent ACC policy.

Suggested citation:

Makes Sense & Safe Surfer. (2025). The Digital Sexual Landscape and Children and Young People in Aotearoa New Zealand
What is it, how are children and youth engaging with it, and how do we keep them safe?

Makes Sense
makessense.org.nz

Safe Surfer
safesurfer.io

The Light Project
thelightproject.co.nz

