NEW ZEALAND CHILD INTERNET SAFETY ACT

Protecting Minors From Harmful Online Content in New Zealand

Submitted to: The Government of New Zealand
Submitted by: Rob Cope, Director & Founder of Our Kids Online
Date: 09 March 2025

Title of Act: New Zealand Child Internet Safety Act

Contents

1. Title of the Act

New Zealand Child Internet Safety Act

2. Purpose

To protect minors (under 18) from exposure to harmful and illegal online content by requiring the implementation of age-appropriate internet filtering, parental controls, and responsible oversight by internet service providers (ISPs), public networks, and device manufacturers.

3. Current Legislative Gaps

3.1 Inadequate Age Restrictions

Existing Law: The Crimes Act 1961, particularly Section 124B, criminalises indecent communication with individuals under 16 years old, leaving those aged 16 and 17 without clear protections from harmful and illegal online content.

Shortfall: This law does not extend protections to all minors under 18, creating a gap where older teenagers remain vulnerable.

3.2 Limited Accountability for Internet Service Providers (ISPs) and Online Platforms

Existing Law: The Digital Child Exploitation Filtering System (DCEFS) operates under the Films, Videos, and Publications Classification Act 1993 to block access to child sexual abuse material.

Shortfall: Participation in DCEFS by ISPs is voluntary, and there is no requirement for broader content filtering. This lack of mandatory safeguards leaves children exposed to a vast and unregulated digital landscape, where they can easily encounter harmful, illegal, exploitative, and inappropriate content. Without accountability, ISPs are not incentivised to implement protective measures, placing young internet users at unnecessary risk.

3.3 Lack of Regulations on Digital Violent Extremism

Existing Law: The Films, Videos, and Publications Classification Act 1993 criminalises the distribution and possession of objectionable material, including certain forms of extremist content.

Shortfall: This law does not comprehensively address online radicalisation or mandate proactive measures for ISPs and platforms to detect and remove extremist content before it reaches minors.

3.4 "Awful but Lawful" Content

Existing Law: The Films, Videos, and Publications Classification Act 1993 criminalises objectionable content but does not regulate harmful yet technically legal material.

Shortfall: The Department of Internal Affairs (DIA) Transparency Report highlights the presence of legally accessible but harmful content, including gore and animal cruelty, which remains unregulated and widely available. This "awful but lawful" content poses significant risks to minors and requires further regulatory attention.

3.5. Reactive Rather than Proactive Measures

Existing Law: The Harmful Digital Communications Act 2015 provides a legal framework for addressing cyberbullying and online harassment.

Shortfall: The Act does not impose obligations on ISPs or online platforms to implement preventative content filtering or age restrictions, instead relying on individuals to report harm after exposure.

4. Definitions

Unfiltered Internet Access: Any unrestricted, unsupervised access to the internet where no parental controls, content filtering, or child protection measures are in place.

Minor: Any individual under the age of 18 years.

Internet Service Provider (ISP): Any business or entity providing internet access to the public.

Public Network Provider: Any business, institution, or entity providing free or paid public internet access.

Device Manufacturer & Retailer: Any business involved in selling internet-enabled devices to consumers.

Parental Control System: A technology-enabled solution that restricts access to harmful online content, including but not limited to, pornography, graphic violence, animal cruelty, gore and exploitative material. This includes illegal online content.

5. Responsibilities and Requirements

5.1. Obligations for Internet Service Providers (ISPs)

(a) ISPs must ensure that every residential internet connection is equipped with a router that includes built-in child-safe filtering technology. By default, these routers must provide two simultaneous internet access options: a filtered connection for children and an unfiltered connection for adults. This ensures that all households have an immediate, built-in ability to protect minors from harmful and illegal online content. Additionally, there must be an option for households that wish to have only filtered internet throughout the home, with no unfiltered access available. This allows families who prioritise a fully protected online environment if they wish.

(b) ISPs must provide two distinct types of SIM cards:

(i) A filtered SIM card for all minors (under 18).

(ii) An unfiltered SIM card available only to those aged 18 and above, requiring proof of age at purchase.

(c) ISPs must continuously upgrade and refine filtering technology to block access to illegal content and content that is harmful to minors, including but not limited to, pornography, graphic violence, animal cruelty, gore and exploitative material.

(d) Failure to comply with these mandatory provisions will result in significant fines and regulatory sanctions to enforce accountability and adherence to child protection measures.

5.2. Obligations for Public Network Providers (Schools, Libraries, Businesses, etc.)

(a) All public Wi-Fi networks accessible by children must have mandatory content filtering enabled.

(b) Schools and educational institutions attended by minors must ensure that all internet-connected devices provided to students are equipped with child-safe browsing settings by default, ensuring a secure and age-appropriate online experience.

(c) Any business, local council, or government entity providing free or paid public internet must apply a child-safe browsing filter to their networks to protect minors from illegal and harmful content.

(d) Failure to comply will result in fines and potential internet service restrictions.

5.3. Obligations for Device Manufacturers & Retailers

(a) Manufacturer Requirements

(i) All manufacturers of internet-enabled devices with web browsing capabilities, including but not limited to smartphones, tablets, computers, and gaming consoles, are legally required to offer models with mandatory built-in internet filtering for minors.

(ii) These filters must be pre-installed and unable to be removed by the purchaser, ensuring a secure and safe online experience for underage users.

(iii) Only manufacturers or authorised retailers may disable or adjust these filters under verified conditions to prevent minors from bypassing protective measures, reinforcing a secure digital environment for young users.

(iv) Manufacturers must continuously upgrade and refine filtering technology to block access to illegal content and content harmful to minors, including but not limited to, pornography, graphic violence, animal cruelty, gore and exploitative material.

(b) Retailer Requirements

(i) All retailers must stock both filtered and unfiltered options for smartphones, tablets, computers, gaming consoles, and any internet-enabled devices with web browsing capabilities sold in New Zealand, ensuring consumers have access to both choices.

(ii) Individuals under the age of 18 may only purchase approved filtered devices by default.

(iii) The sale of unfiltered devices to minors is strictly prohibited and will be met with penalties for non-compliance.

(iv) All retailers must stock both 18+ SIM cards and filtered SIM cards for minors (under 18) to ensure consumers in New Zealand have access to both choices.

(v) Retailers may only sell 18+ SIM cards with verified proof of age, ensuring minors cannot obtain unfiltered access.

(vi) The sale of 18+ SIM cards to minors is strictly prohibited and will be met with penalties for non-compliance.

5.4. Obligations for Parents & Guardians

(a) Active Monitoring and Screen Time Limits

Parents and guardians have a duty of care to actively monitor their children's online activities, enforce safe browsing habits, and establish healthy screen time limits. They must take proactive measures to ensure a balanced and secure digital environment that promotes both online safety and well-being.

(b) Safe Internet Access

(i) Parents and guardians have a duty of care to ensure that minors under their care can only access filtered internet. They must actively configure home networks and devices with secure access controls, such as passwords or PINs, to prevent unauthorised access to unfiltered content. This duty includes preventing circumvention of filtering measures and maintaining a safe digital environment at home.

(ii) Parents and guardians have a duty of care to ensure that all devices minors have access to, which require a SIM card, including but not limited to mobile phones, smartphones, smartwatches, and tablets are equipped with a filtered SIM. This includes replacing any existing SIM card with the new filtered SIM card to guarantee a safe and secure online experience for children.

(c) Government Support

Government agencies will provide educational resources, tools, and training to help parents meet these obligations effectively, including best practices for managing children's digital access.

(c) Legal Consequences

Parents who knowingly expose children to illegal and harmful online content through negligence may be subject to counselling orders or civil penalties in extreme cases where harm is proven.

(d) Failure to Implement Controls

Parents who fail to implement reasonable parental controls in the home, including ensuring that all SIM-enabled devices used by minors (under 18) have a filtered SIM, may be subject to increased scrutiny or intervention by child welfare agencies.

6. Penalties for Non-Compliance:

(a) **ISPs:** Fines up to NZD 500,000 for failure to implement content filtering.

(b) **Device Manufacturers & Retailers:** Fines up to NZD 250,000 for non-compliance with default parental control settings.

(c) **Public Network Providers:** Subject to fines of up to NZD 10,000 for non-compliance with default parental control settings.

(d) **Individuals:** Any individual who supplies a minor (under 18) with an 18+ SIM card or unfiltered access to the internet will face penalties. An Infringement Notice with a fee of up to NZD 2,000. Upon conviction, a fine of up to NZD 10,000.

7. Implementation & Oversight:

(a) An Online Harm Prevention Unit for Children will be established to oversee enforcement, monitoring, and updates to regulations.

(b) This unit will work in collaboration with law enforcement, online safety experts, child welfare organisations, educational institutions and any other relevant agencies or organisations to ensure compliance and effectiveness.

(c) The unit will be responsible for providing guidelines and technical support to ISPs, device manufacturers, retailers, and public network providers to facilitate the implementation of content filtering and safety measures.

(d) The government will allocate resources for ongoing research into online harms affecting minors and develop adaptive solutions to emerging digital threats.

(e) A public education campaign will accompany the law to help parents, schools, and businesses comply and understand best practices.

8. Review and Future Adaptations:

(a) The law will be reviewed every three years to assess its effectiveness and adapt to emerging digital trends.

(b) Stakeholders, including parents, educators, tech experts, and youth representatives, will contribute to future amendments.

9. Conclusion:

This Act aims to balance child safety, parental responsibility, and digital freedom while ensuring that minors are not inadvertently exposed to illegal and harmful content online. By placing responsibility on ISPs, businesses and strengthening parental obligations, we can create a safer digital environment for children and youth in New Zealand.

I request that this proposal be considered for introduction as a government bill or incorporated into ongoing legislative reviews concerning online safety.

Signed

Rob Cope

Our Kids Online

admin@ourkidsonline.info