

A photograph of two women in the foreground, both looking down at their smartphones. The woman in the foreground has long dark hair and is wearing a black top and a gold chain necklace. The woman behind her is wearing glasses and a white jacket. The background is blurred, suggesting an indoor setting with other people.

tuanz

TECH USERS ASSOCIATION

**Navigating the Social Media Age-
Gating Debate: A Discussion Paper
from Tech Users NZ.**

June 2026

**Encouraging an open, evidence-based national
dialogue.**

Executive Summary

The rapid integration of digital technologies into daily life has initiated a global regulatory shift toward age-gating social media platforms, driven by concerns over child safety, mental health, and the impact of algorithmic designs on youth.¹ This paper maps the shifting international and domestic landscapes as Aotearoa New Zealand navigates this complex debate. While several countries have enacted or proposed legislative measures to restrict social media access for minors under the age of 16, New Zealand has entered a critical period of deliberation.³ In mid-May 2026, the Government paused progress on a prominent private member's bill that sought to introduce a mandatory under-16 ban.³ This decision was made to allow the Government to evaluate a more comprehensive, system-level policy approach to online harm under the leadership of the Ministry of Education.⁵

The policy debate in New Zealand presents a fundamental tension between two primary philosophies: a protective, exclusion-based framework that seeks to insulate young people from digital spaces, and a rights-based, "safety-by-design" approach that focuses on systemic platform accountability.⁷ Proponents of an outright ban point to severe mental health impacts, algorithmic addiction, cyberbullying, and commercial exploitation as justifications for state intervention.¹ Conversely, youth advocates, civil society groups, and regulatory bodies caution that blunt age-gating mechanisms pose profound risks to user privacy, introduce severe cybersecurity vulnerabilities, and threaten to isolate vulnerable or marginalised youth who rely on online networks for peer support and community.⁷

In considering the policy options, TUANZ believes the following principles should guide decision-making:

- **Proportionality:** interventions should balance safety objectives with privacy, access, and innovation impacts
- **Practicality and enforceability:** solutions must be workable in a New Zealand context and resilient to circumvention
- **Platform accountability:** responsibility should sit appropriately with those best able to manage risk
- **Equity and inclusion:** policies should not disproportionately disadvantage vulnerable groups
- **Future-proofing:** frameworks should remain adaptable to rapid technological change

These principles are reflected in the core questions for the national debate set out at the end of this document, which are designed to help decision-makers navigate the key trade-offs and design considerations in a New Zealand context.

The Global Landscape

The international approach to regulating social media access for minors is highly fragmented, characterised by differing levels of platform liability, technological standards, and enforcement mechanisms. Distinct models are emerging from Australia, the United Kingdom, the European Union, and the United States.

Jurisdiction	Primary Regulatory Vehicle	Age Threshold	Core Mechanism	Maximum Enforcement Penalties
Australia	Online Safety Act 2021 (as amended in 2024) ²	Under 16 ²	Platform duty to take "reasonable steps" to block accounts; no parental consent exceptions. ²	Up to A\$49.5 million per corporate violation. ²
United Kingdom	Online Safety Act 2023 ¹²	Varies (under 18 for high-risk content) ¹⁴	"Highly effective" age verification/estimation to prevent access to harmful content. ¹²	Up to 10% of qualifying global annual revenue. ¹²
European Union	Digital Services Act (DSA) ¹⁶	Varies by Member State (e.g., France under 15, Austria under 14) ¹⁸	Systemic minor protection, algorithmic risk mitigation, and harmonised privacy-preserving age-verification tools. ¹⁶	Up to 6% of global annual revenue.
United States	Evolving State Statutes (e.g., California AB 1043) ¹⁹	Varies (e.g., under 13, 13–16, 16–18) ¹⁹	Shift toward device-level and operating system (OS) age-gating and app store accountability. ²⁰	Varies; subject to intense constitutional litigation. ²⁰

Australia's Under-16 Ban: Early Lessons and Enforcement Friction

At the forefront of the international landscape is Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024, which passed on November 29, 2024, and received Royal Assent on December 10, 2024.⁴ The origins of this policy trace back to November 2023, when Shadow Communications Minister David Coleman introduced a trial bill for age-verification technology.⁴ Although that initial bill was unsuccessful, it prompted the

Albanese Government to fund an age-assurance trial in the 2024 federal budget, which was followed by a pledge from Opposition Leader Peter Dutton to implement an under-16 ban within his first 100 days in office.⁴

Following a transitional period, the minimum age obligation officially took effect on December 10, 2025.² The regulatory architecture places the legal burden entirely on platforms to take "reasonable steps" to prevent Australians under 16 from maintaining accounts, explicitly exempting child users and their parents from any penalties.² Corporate non-compliance carries civil penalties of up to 150,000 penalty units, equivalent to A\$49.5 million.² On July 29, 2025, the Minister for Communications established the Online Safety (Age-Restricted Social Media Platforms) Rules 2025 (amended in March 2026), which clarify that the under-16 restrictions apply to services like Facebook, Instagram, Snapchat, TikTok, X, Threads, Twitch, Kick, Reddit, and YouTube.² However, the rules exclude standalone messaging, online gaming, professional networking, education, and health support applications.¹¹

To support implementation, the eSafety Commissioner published regulatory guidance on September 16, 2025, alongside a national campaign titled "For the good of their wellbeing," which launched on October 19, 2025.² To assess the long-term societal and psychological outcomes of this legal shift, eSafety appointed an academic advisory group led by Stanford University in late September 2025.²

Early implementation data has highlighted several significant friction points. By mid-December 2025, age-restricted platforms reported removing approximately 4.7 million accounts belonging to users under 16 across Australia.² Ahead of the enforcement deadline, Meta transitioned its platforms (Instagram, Facebook, and Threads) to require facial scanning or official identity document uploads to verify age.⁴ Despite these actions, youth advocacy organisations note that eSafety data reveals approximately two-thirds of the target demographic remain on supposedly banned platforms through circumvention methods.⁷ Furthermore, the final report of the Australian Government's Age Assurance Technology Trial, released on August 1, 2025, confirmed that while modern age estimation and verification technologies can be highly private and robust when deployed correctly, they continue to face practical limitations regarding user friction and systemic reliability.²

Other International Frameworks: United Kingdom, European Union, and United States

In the United Kingdom, the regulatory framework has shifted away from direct social media access bans to a content-gate model established by the Online Safety Act 2023.¹² The legislation places a statutory duty on online services likely to be accessed by children to implement "highly effective" age verification or age estimation measures to ensure minors are shielded from harmful materials, including pornography, suicide promotion, and self-harm content.¹² Under this model, the Digital Economy Act 2017's original age-verification proposals were repealed.¹⁵

The UK safety regime took effect in phases: the Section 81 duty on adult platforms (Part 5 services) commenced on January 17, 2025, immediately following the publication of Ofcom's final age assurance guidance.¹⁴ On April 24, 2025, Ofcom laid its child safety codes of practice in Parliament, requiring in-scope platforms to complete comprehensive risk

assessments by July 24, 2025.¹⁴ Ofcom has defined an outcome-based standard for what constitutes "highly effective" age assurance, assessing technologies based on technical accuracy, robustness against circumvention, reliability, and fairness.¹² Approved methods include Open Banking verification, photo ID matching, facial age estimation, and mobile network operator checks.¹²

By February 2026, Ofcom had launched formal investigations into more than 90 services, issuing six financial penalties for non-compliance.¹² These included a £1 million fine against an adult website operator in December 2025 and an £800,000 fine against Kick Online Entertainment in February 2026.¹² In early 2026, investigations were expanded to cover generative artificial intelligence platforms, including X's Grok AI chatbot and Joi.com.¹²

Furthermore, on March 12, 2026, Ofcom issued letters to major technology platforms requiring them to enforce their minimum age policies using highly effective age assurance, setting a reporting deadline of April 30, 2026.¹³ To support enforcement, the Information Commissioner's Office (ICO) and Ofcom released a joint statement on March 26, 2026, addressing the intersection of online safety and data protection.¹³

In their latest move on June 15, 2026, UK Prime Minister Keir Starmer announced that the British Government will introduce a comprehensive, mandatory social media ban for all children under the age of 16. Drawing directly on public feedback from over 116,000 national consultation responses which revealed that 9 in 10 parents support an outright ban, the upcoming framework explicitly targets platforms such as TikTok, Instagram, Snapchat, Facebook, YouTube, and X. Billed as an "Australia Plus" model, the UK's architecture will go beyond a simple platform block to institute system-level restrictions: it mandates the complete deactivation of high-risk features by default for minors, including livestreaming and communication with strangers across online gaming networks. Furthermore, the regulations clamp down on generative artificial intelligence, forcing a strict minimum age threshold of 18 for any AI "romantic companion" chatbots or tools capable of explicit interactions. Backed by legislative powers under the Children's Wellbeing and Schools Act, the Government plans to lay the regulations before Parliament before Christmas, with full, Ofcom-enforced compliance deadlines slated to come into force in Spring 2027.

The European Union's approach integrates compliance under the Digital Services Act (DSA) with centralized, privacy-focused technological solutions.¹⁶ Article 28(1) of the DSA mandates that platforms accessible to minors implement appropriate and proportionate measures to ensure high levels of privacy, safety, and security.¹⁷ Under Articles 34 and 35(1), Very Large Online Platforms (VLOPs) and Online Search Engines (VLOSEs) must continuously assess and mitigate risks to minors.¹⁷ The European Commission has actively utilised these powers: in early 2026, Snapchat was investigated over suspected failures in age assurance, grooming prevention, and the dissemination of prohibited products.¹⁷ Similarly, Meta was investigated in April 2026 for failing to prevent minors under 13 from accessing its platforms.¹⁷

To prevent a fragmented landscape across Member States such as France's under-15 social media ban, Austria's proposed under-14 limit, and emerging restrictions in Greece and Ireland, the European Commission announced on April 15, 2026, that its harmonised, open-source age-verification mobile application was "technically ready".¹⁸ Developed under contract by Scytāles and T-Systems, this "mini wallet" is designed to align with the technical specifications of the European Digital Identity Wallet, scheduled for deployment by the end of

2026.¹⁶ By utilising Zero-Knowledge Proofs (ZKPs) and electronic ID data, the app allows users to prove they meet specific age thresholds by transmitting a simple "true/false" signal without revealing their name, exact date of birth, or online activity.¹⁶

Under Directive 2015/1535, EU Member States are legally required to notify the Commission of draft technical regulations including national social media bans before adoption.¹⁷ This triggers a mandatory three-month standstill period for cooperative dialogue.¹⁷ Under Court of Justice of the European Union (CJEU) case law (*CIA-Security* and *Unilever*), any national restriction adopted without this prior notification is rendered completely unenforceable in domestic proceedings.¹⁷

In the United States, legislation regarding social media age verification has expanded rapidly at the state level since Utah passed the Utah Social Media Regulation Act in March 2023.²⁴ In 2025, nine states implemented age-verification laws for accessing specific content (including South Carolina, Florida, Tennessee, Georgia, Wyoming, North Dakota, Arizona, and Ohio).²⁰ However, these state-level statutes have faced legal challenges from industry associations like NetChoice on First Amendment, preemption, and vagueness grounds.²¹ For example, the Protect Tennessee Minors Act remains on hold pending the outcome of the federal case *Free Speech v. Paxton*.²⁵ In South Carolina, NetChoice filed suit on February 9, 2026, seeking a preliminary injunction by March 9, 2026.²¹ On March 12, 2026, the Ninth Circuit Court of Appeals issued a decision in *NetChoice v. Bonta* regarding California's Age-Appropriate Design Code Act, finding that standards framed around subjective concepts like a child's "best interests" or "well-being" failed to provide constitutionally adequate notice of prohibited conduct.²¹

These legal challenges have prompted a shift toward device-level and operating system (OS) age-gating.²⁰ California's Digital Age Assurance Act (AB 1043), taking effect on January 1, 2027, requires operating systems (including Windows, macOS, Android, ChromeOS, and Linux distributions) to prompt users for their age during device setup and transmit a standardised age signal (under 13, 13–16, 16–18, or over 18) to installed applications.¹⁹ While California's statute accepts self-attestation, digital rights groups warn that OS providers may eventually implement strict identity verification to avoid liability.¹⁹ In tandem, states like Texas, Utah, Louisiana, and Alabama (via House Bill 161 in February 2026) have enacted app store accountability bills that place parental consent and age verification duties directly on app store providers.²¹ At the federal level, the Parents Decide Act, introduced in April 2026, proposed nationwide, mandatory OS-level birth date registration for all users, alongside Federal Trade Commission (FTC) oversight of parental verification standards.¹⁹

These international approaches highlight the trade-offs between enforceability, privacy, and effectiveness, and reinforce the need for solutions that are proportionate and achievable within New Zealand's regulatory scale.

The New Zealand Context: Legislative & Political Landscape

Aotearoa New Zealand's domestic policy debate has evolved through competing private member's bills, a comprehensive select committee inquiry, and clear political divisions.³

Catherine Wedd's Social Media (Age-Restricted Users) Bill

In May 2025, National Party MP Catherine Wedd announced a private member's bill, the *Social Media (Age-Restricted Users) Bill*, designed to bar children under 16 from accessing social media.³ Following its drawing from the parliamentary ballot on October 23, 2025, the Bill proposed a legal framework requiring social media providers to take "all reasonable steps" to prevent underage users from maintaining accounts.³ The Bill allowed courts to impose civil pecuniary penalties on non-compliant platforms, while exempting minors and parents from liability.³

Wedd noted that her motivation stemmed from her experience as a parent of four children, alongside the passage of Australia's Online Safety Amendment.³ Because National's coalition partner, the ACT Party, refused to support the measure as a Government bill, National advanced it as a member's bill, with Prime Minister Christopher Luxon seeking cross-party support.³ In November 2025, Luxon reiterated his commitment to introducing age-restricting legislation before the 2026 general election, tasking Education Minister Erica Stanford with reviewing implementation lessons from Australia.³

However, in mid-May 2026, the Government paused work on the Bill.³ Minister Stanford clarified that the member's bill was being deprioritised to allow the Government to progress a broader, more integrated program of work addressing social media harms and systemic online safety.⁶ While the Prime Minister's office confirmed that introducing legislation before the next election remains a target, the legislative future of an outright under-16 ban remains uncertain.⁶

The Select Committee Inquiry on Online Harm

At the request of ACT MP Parmjeet Parmar, Parliament's Education and Workforce Committee, led by National MP Carl Bates, conducted a detailed inquiry into youth online harm.³ Initiated in July 2025, the inquiry received 430 submissions from 400 organizations and individuals, alongside 87 in-person testimonies.³ On December 10, 2025, the Committee released an interim report³, followed by its final report on March 5, 2026.²⁷

The final report concluded that online harm is a fast-moving, global issue that requires a coordinated, public-health-aligned response.²⁷ The Committee issued 12 core recommendations, which included:

1. Reviewing existing legislative frameworks, including the *Films, Videos, and Publications Classification Act 1993* and the *Harmful Digital Communications Act 2015*,

- to resolve regulatory overlaps.¹⁰
2. Establishing an independent national online safety regulator.¹⁰
 3. Introducing age restrictions for social media platforms.³⁰
 4. Banning web- and device-based "nudify" applications and prohibiting the creation and distribution of non-consensual deepfake sexual imagery (aligning with separate legislative efforts like Laura McClure's deepfake member's bill).²⁸
 5. Regulating and mandating transparency for algorithmic recommendation systems.¹⁰
 6. Enhancing digital literacy education and empowering parents and caregivers.³⁰

Political Dividing Lines in Parliament

The New Zealand Parliament is divided along clear ideological lines regarding the necessity and feasibility of an outright under-16 social media ban.³

- **The National Party** remains conceptually supportive of age-restriction legislation, emphasising the need to protect young people from cyberbullying, mental health decline, and algorithmic exploitation.¹ National supports a "fast-follower" approach to build on international regulatory evidence.²⁷
- **The Labour Party** supports age-restricting measures but argues that the primary regulatory burden must be placed on the platforms rather than individual users.³ Reuben Davidson (Labour) drafted a matching member's bill proposing \$50,000 fines for social media providers that fail to restrict "harmful content".³ Labour has strongly advocated for the mandatory regulation of algorithmic recommendation engines.¹⁰
- **ACT New Zealand** and **The Green Party** formally opposed the Select Committee's recommendation to introduce mandatory under-16 age restrictions, releasing dissenting views.³ Both parties argue that age restrictions are technically easy to circumvent, risk isolating vulnerable youth, and fail to address the underlying design features that affect users of all ages.³
- **ACT and the Greens** have also strongly opposed any potential domestic regulation of Virtual Private Networks (VPNs) or the introduction of intrusive digital identity cards.³ They note that VPNs are critical tools for business operations, data security, and privacy protection against state or corporate surveillance.¹⁰

To put this debate in context, InternetNZ's 2025 research, alongside the *World Internet Project New Zealand 2025* report, highlights the digital habits of New Zealanders:

Metric	Detail / Findings
High Personal Internet Use	47% of online New Zealanders spend four or more hours daily on the internet, rising to 63% for those aged 18–29. ²⁹
Experience of Online Harm	15% of all surveyed New Zealanders report experiencing online harm or harassment. ²⁹
Māori and Pacific Community Concerns	80% of Pacific peoples and 64% of Māori are highly concerned about the use of the internet to spread dangerous or discriminatory messaging. ²⁹
Declining Public Optimism	The proportion of New Zealanders who believe the positives of the internet outweigh the negatives fell from 80% in 2023 to 72% in 2025. ²⁹

Domestic Stakeholder Perspectives

The public debate within Aotearoa New Zealand is shaped by highly active civil society organisations, regulatory bodies, parental groups, and youth advocates. The following is our summarisation and should not be taken as being a full description of their positions.

Parental Advocacy and Protective Groups

A prominent segment of parental advocates and grassroots organisations continues to lobby for an outright under-16 social media ban.³ These groups represent a growing public concern over what they characterise as an unregulated public health crisis affecting young people.¹ Their arguments emphasise:

- **Addiction and Mental Health:** Proponents argue that modern social media platforms utilise predatory design patterns such as infinite scroll and account-based algorithmic recommendations which are specifically engineered to exploit developmental vulnerabilities in children, leading to sleep deprivation, severe anxiety, and depression.²
- **The Household Burden:** Parents express frustration with the "asymmetry of power" between isolated families and multi-billion-dollar technology platforms.⁷ They argue that device-level parental controls are technically complex, easily bypassed by digital-native children, and create continuous domestic friction.⁹ Under this view, a state-mandated ban provides necessary symbolic and practical leverage, shifting the collective societal standard of what is acceptable.⁹

Youth and Rights-Based Advocacy

In contrast, a collaborative group of children's rights organisations including Children's Commissioner Dr. Claire Achmad, the Children's Convention Monitoring Group (CMG), Save the Children New Zealand, and UNICEF Aotearoa, argue that a blunt access ban fails to make the internet safer while actively violating children's rights.⁷

In a series of reports released in June 2026, Commissioner Achmad emphasised the importance of centering the "Mokopuna Voice" in policymaking, noting that children have a statutory right under the United Nations Convention on the Rights of the Child (UNCRC) to be heard in decisions affecting their lives.⁵ These advocacy bodies raise several key concerns:

- **The Risk of Sudden Isolation:** Digital environments are fundamental to modern youth socialisation.⁵ For geographically isolated rural youth, disabled children, and those with chronic health conditions, social media platforms are essential tools for maintaining connection, pursuing self-directed learning, and accessing educational resources.⁷
- **Disproportionate Impact on Rainbow Youth:** Online communities are particularly critical for marginalised groups, such as Rainbow (LGBTIQA+) and Māori mokopuna, who frequently use social media to find peer support, build a sense of belonging, and escape unsupportive physical environments.⁷ Restricting access to these networks can exacerbate mental health challenges rather than alleviate them.⁷

- **Shifting the Burden of Safety:** Human rights agencies reject the logic of absolute exclusion, arguing that society does not simply hand young people car keys at age 16 without prior instruction.³² Instead, they advocate for structured, age-appropriate digital citizenship education to build resilience and navigation skills from an early age.⁷

Policy Options for Aotearoa New Zealand

This section outlines three distinct policy pathways. These options are not mutually exclusive. Most jurisdictions are moving toward hybrid models that combine elements of access restrictions, platform accountability, and user empowerment.

Option A: The Under-16 Exclusion Model (A Hard Age Ban)

This approach mirrors the Australian legislation and Catherine Wedd's original member's bill, imposing a strict legal prohibition on platforms allowing individuals under 16 to create or hold accounts.²

- **Pros / Intended Benefits:**

- Establishes a clear, enforceable legal standard across the entire digital sector, relieving parents of the individualised burden of policing device access.¹
- Motivates rapid compliance from global technology platforms by introducing severe financial penalties (e.g., civil fines modeled on Australia's A\$49.5 million or the UK's 10% global revenue standard).²
- Provides a strong symbolic, state-backed mandate that shifts social norms and encourages youth to engage in healthier offline and physical activities.¹

- **Cons / Implementation Challenges:**

- **Privacy Risks:** Requires highly intrusive verification mechanisms (such as uploading government IDs, credit card checks, or biometrics), creating targets for data breaches and commercial exploitation.¹⁰
- **Inevitability of Circumvention:** The technical ease of using VPNs, falsified accounts, or proxy servers ensures that a significant percentage of minors will continue to access platforms, often pushing them to less-regulated, darker online spaces.²³
- **Vulnerability of Marginalised Youth:** Inevitably cuts off disabled, rural, and Rainbow youth from vital support groups and safe online environments.⁷

Option B: The Structural Reform Model (Co-Regulation & Safety-by-Design)

This approach shifts the regulatory focus entirely away from individual access bans toward the systemic, algorithmic architecture of the platforms, as advocated by UNICEF and the CMG.⁷

- **Pros / Intended Benefits:**

- Targets the root causes of online harm specifically predatory features like infinite scroll, non-consensual deepfake generation, and addictive algorithmic recommendation loops, rather than blaming the child.²⁹

- Preserves children's rights to information, expression, and peer community, while keeping marginalised groups connected to essential safety nets.⁷
- Avoids the necessity of establishing highly intrusive, state-wide digital identity or age-gating verification systems that threaten user privacy.¹⁰
- **Cons / Implementation Challenges:**
 - **Regulatory Complexity:** Designing, auditing, and enforcing algorithmic compliance and transparency is technically demanding, requiring substantial, long-term state funding and highly specialised technical expertise.¹⁰
 - **Jurisdictional Limits:** Regulating the proprietary algorithms of multi-trillion-dollar offshore technology corporations (e.g., Meta, ByteDance, Alphabet) poses major enforcement challenges for a small nation-state like New Zealand.²⁷
 - **Delayed Impact:** Systemic engineering and platform architecture overhauls take years to fully implement, offering no immediate relief to parents demanding instant solutions.¹⁸

Option C: The Empowered User and Educational Model (Device-Level & Literacy Controls)

This model focuses on device-level settings, OS-level age signal transmission (akin to California's AB 1043), and mandated state-funded digital literacy frameworks.¹⁹

- **Pros / Intended Benefits:**
 - Minimises platform-level data collection by allowing parents and users to declare and manage age parameters directly on physical devices (such as smartphones and operating systems) during initial setup.¹⁹
 - Equips children and families with systemic, lifelong digital resilience and navigation skills rather than relying on blunt, temporary state bans.⁷
 - Maintains high alignment with international data privacy and open-internet standards, avoiding constitutional, human rights, or free speech challenges.²¹
- **Cons / Implementation Challenges:**
 - **Inequality of Digital Literacy:** The effectiveness of this model relies heavily on the time, technical capability, and resources of parents and caregivers, risking worse safety outcomes for children in structurally disadvantaged households.⁷
 - **Enforcement Dispersal:** Relies on device manufacturers (e.g., Apple, Google, Microsoft) implementing consistent, honest age-bracket application programming interfaces (APIs), which can still be bypassed if not backed by strict state oversight.¹⁹
 - **Unregulated Content Ecosystems:** Leaves the underlying platform architectures, click-bait economics, and harmful content feeds completely untouched.³²

Policy Spectrum Comparison

To assist in evaluating these three strategic pathways, the following table compares the options across core operational, technical, and social indicators.

Each policy pathway carries different implications for regulatory capability, resourcing, and time to impact. Decision-makers will need to consider not only the effectiveness of each approach, but the practical requirements for implementation and ongoing enforcement within New Zealand's institutional context.

Indicator	Option A: Under-16 Exclusion Model	Option B: Structural Reform Model	Option C: Empowered User Model
Primary Regulatory Target	Individual user access and platform age-gates. ²	Systemic platform architecture, algorithms, and features. ¹⁰	Device operating systems, parental controls, and education. ⁷
Primary Burden of Compliance	Shared between platforms (enforcement) and families (verification). ¹⁰	Placed exclusively on digital platforms and algorithmic systems. ⁷	Placed on device manufacturers and individual households. ⁹
Data Privacy Footprint	High Risk: Requires mass collection/processing of sensitive identity data. ¹⁰	Low Risk: Minimizes personal identification; focuses on anonymised design. ¹⁷	Moderate Risk: Confines age data to local devices, though OS providers may verify. ¹⁹
Technical Circumvention Vulnerability	Extremely High: Easily bypassed via standard VPNs or fake credentials. ²³	Low: System-level changes (e.g., feed design) cannot be bypassed by users. ³²	High: Children frequently bypass local parental settings and filters. ⁹
Impact on Marginalized/Vulnerable Youth	High Risk: Potential acute isolation and loss of peer networks. ⁷	Positive: Enhances platform safety while preserving essential access. ⁸	Neutral/Variable: Dependent entirely on the support structures of the home. ²⁹

Core Questions for the National Debate

As New Zealand policy-makers, families, and technology users engage with this ongoing policy review, several critical questions are core to the debate.

Framing the Problem

- To what extent is government intervention in children's access to social media necessary or appropriate?
- What specific harms should policy prioritise addressing, and for whom?
- What outcomes should any intervention seek to achieve (e.g. improved safety, reduced harm exposure, preserved access to information and connection)?

Policy Approach

- Which policy approach, or combination of approaches, is most appropriate for New Zealand?
 - Age-based restrictions on access
 - Platform design and safety-by-design regulation
 - Device-level controls and parental tools
 - Education and digital literacy
- What factors should guide the choice between restriction, regulation, and education-based approaches?

Trade Offs

- How should policy balance competing objectives such as:
 - Child safety and wellbeing
 - Privacy and data protection
 - Access to information and participation
 - Individual, parental, platform, and state responsibility
- Are there trade-offs that should be prioritised over others in the New Zealand context?

Technical Feasibility & Privacy

- What should constitute reasonable and proportionate age assurance in a New Zealand context?
- What level of identity verification or data collection would be acceptable to support this?
- How should policy balance safety objectives with privacy, cybersecurity, and data protection risks?
- How should New Zealand respond to likely circumvention behaviours (e.g. VPN use), given their legitimate role in business and personal security?
- What role, if any, should device-level or operating system controls play relative to

platform-level solutions?

Equity & Inclusion

- How can policy ensure that efforts to reduce harm do not unintentionally exclude vulnerable groups from important online communities?
- Are there risks that restrictions could displace harm (e.g. to less regulated or offshore platforms), and how should this be managed?
- How should policy account for the different needs and experiences of young people, including rural, disabled, Māori, Pacific, and Rainbow youth?
- What role should Te Tiriti o Waitangi obligations play in shaping online safety policy?

Platform Accountability

- Where should the primary responsibility for online safety sit - platforms, government, parents, or a combination?
- What enforcement mechanisms would be credible, proportionate, and effective for a country of New Zealand's size and regulatory reach?
- How can regulation ensure platform accountability while avoiding unnecessary barriers to innovation, access, or competition?
- How should any regulatory framework remain agile and responsive to emerging technologies (e.g. AI and deepfake tools) while protecting fundamental rights?

Implementation and success

- What would successful policy intervention look like in practice?
 - How should success be measured and monitored over time?
 - What level of cost, complexity, and compliance burden would be acceptable to achieve policy objectives?
 - How should responsibilities and resourcing be distributed across government, regulators, industry, and households?
-

TUANZ: Championing a Brighter Digital Future for every New Zealander



The Technology Users Association of New Zealand (TUANZ) is the voice of technology users in Aotearoa New Zealand. Established as a not-for-profit organisation, TUANZ acts as the independent group representing the interests and needs of individuals, businesses, and organizations as they navigate the evolving technology landscape.

Our membership encompasses a diverse range of technology users, from small businesses and innovative startups to large enterprises and public sector entities. This broad network connects those who utilise technology to achieve their goals, fostering a community dedicated to understanding, adopting, and maximising the benefits of digital tools and services.

TUANZ plays a crucial role in bridging the gap between technology providers and end-users. We work collaboratively across sectors, engaging with government, industry, and the wider community to ensure that technology deployment and policy decisions are user-centric and contribute to a thriving digital ecosystem for all New Zealanders.

Our focus is on empowering technology users through education, advocacy, and the facilitation of meaningful connections. We strive to ensure that New Zealanders can confidently and effectively leverage technology to enhance productivity, innovation, and overall quality of life. We provide a platform for an informed and influential user voice, advocating for policies and practices that support positive technology outcomes for our members and the nation.

Note: This report was developed utilising Google Gemini in Deep Research mode as a first draft, then significantly edited by members of the staff and Board of TUANZ before this release version. The Endnotes provide the references used by the tools to help create the first draft.

Endnotes

1. Social Media (Age-Restricted Users) Bill - Parliament - DRAFT FOR CONSULTATION, accessed on June 15, 2026, <https://bills.parliament.nz/download/ProposedMembersBill/63d21ac9-35e9-4cc8-a323-08dd8c12d81b>
2. Social media age restrictions | eSafety Commissioner, accessed on June 15, 2026, <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>
3. Social Media (Age-Restricted Users) Bill - Wikipedia, accessed on June 15, 2026, [https://en.wikipedia.org/wiki/Social_Media_\(Age-Restricted_Users\)_Bill](https://en.wikipedia.org/wiki/Social_Media_(Age-Restricted_Users)_Bill)
4. Online Safety Amendment (Social Media Minimum Age) Act 2024 - Wikipedia, accessed on June 15, 2026, [https://en.wikipedia.org/wiki/Online_Safety_Amendment_\(Social_Media_Minimum_Age\)_Act_2024](https://en.wikipedia.org/wiki/Online_Safety_Amendment_(Social_Media_Minimum_Age)_Act_2024)
5. Social media ban: Hear kids first, says Commissioner, accessed on June 15, 2026, <https://www.odt.co.nz/news/national/social-media-ban-hear-kids-first-says-commissioner-rnz>
6. Stanford promises update on social media ban in June, accessed on June 15, 2026, <https://www.1news.co.nz/2026/05/16/stanford-promises-update-on-social-media/>
7. Experts urge government to go beyond a ban - Save the Children NZ, accessed on June 15, 2026, <https://www.savethechildren.org.nz/media-hub/experts-urge-government-to-go-beyond-a-ban>
8. Social media ban: Young people must be listened to - commissioner - 1News, accessed on June 15, 2026, <https://www.1news.co.nz/2026/06/14/social-media-ban-young-people-must-be-listened-to-commissioner/>
9. Frustrated parents of under-16s look for help to enforce 'ineffective' social media ban : r/aus, accessed on June 15, 2026, https://www.reddit.com/r/aus/comments/1sohtv4/frustrated_parents_of_under16s_look_for_help_to/
10. Inquiry into youth online harm » InternetNZ, accessed on June 15, 2026, <https://internetnz.nz/news-and-articles/inquiry-into-youth-online-harm/>
11. Social media minimum age | Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, accessed on June 15, 2026, <https://www.infrastructure.gov.au/media-communications/internet/online-safety/social-media-minimum-age>
12. Age Verification Under the UK Online Safety Act: What You Need to ..., accessed on June 15, 2026, <https://oneid.uk/news-and-events/uk-online-safety-act-age-verification-guide>
13. Age Assurance in 2026: what do digital businesses operating in the UK and EU need to know? - Lewis Silkin LLP, accessed on June 15, 2026, <https://www.lewissilkin.com/insights/2026/04/17/age-assurance-in-2026-what-do-digital-businesses-operating-in-the-uk-and-eu-need-to-know>
14. Online Safety Act: explainer - GOV.UK, accessed on June 15, 2026, <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>
15. Online age verification in the United Kingdom - Wikipedia, accessed on June 15, 2026, https://en.wikipedia.org/wiki/Online_age_verification_in_the_United_Kingdom

16. The EU approach to age verification - Shaping Europe's digital future - European Union, accessed on June 15, 2026,
<https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification>
17. The EU Commission's Approach to Age Verification: Mobile Apps ..., accessed on June 15, 2026,
<https://fpf.org/blog/the-eu-commissions-approach-to-age-verification-mobile-apps-dsa-enforcement-and-challenging-national-social-media-bans/>
18. EU's Age Verification App: A Technical Fix for a Fragmented Legal ..., accessed on June 15, 2026,
<https://www.zwillgen.com/eu-uk/eus-age-verification-app-technical-fix-fragmented-legal-landscape/>
19. Your Computer May Soon Require an Age Check. And You Might ..., accessed on June 15, 2026,
<https://www.pcmag.com/explainers/your-computer-may-require-an-age-check-might-have-to-prove-it>
20. The Year States Chose Surveillance Over Safety: 2025 in Review, accessed on June 15, 2026,
<https://www.eff.org/deeplinks/2025/12/year-states-chose-surveillance-over-safety-2025-review>
21. States Push Children's Privacy Laws Forward, Even as Courts Keep Narrowing the Lines, accessed on June 15, 2026,
<https://www.hklaw.com/en/insights/publications/2026/04/states-push-childrens-privacy-laws-forward>
22. Australia's Under-16 Social Media Ban Backed By Age Verification Trial | 10 News First, accessed on June 15, 2026, <https://www.youtube.com/watch?v=TwHX5Phfk1M>
23. The EU's Age Verification Efforts: Child Protection, Privacy, and Digital Identity, accessed on June 15, 2026,
<https://bisi.org.uk/reports/the-eus-age-verification-efforts-child-protection-privacy-and-digital-identity>
24. Online age verification laws by country - Wikipedia, accessed on June 15, 2026,
https://en.wikipedia.org/wiki/Online_age_verification_laws_by_country
25. US Children's Privacy Legislation Tracker | Mayer Brown, accessed on June 15, 2026,
<https://www.mayerbrown.com/en/insights/resource-centers/cybersecurity-and-data-privacy-resource-center/us-childrens-privacy-legislation-tracker>
26. Social Media (Age-Restricted Users) Bill | New Zealand Legislation, accessed on June 15, 2026, <https://www.legislation.govt.nz/bill/member/2025/0216/4.0/whole.html>
27. Final report into youth harm online released by select committee | National Party, accessed on June 15, 2026,
<https://www.national.org.nz/news/20260305-carl-bates-final-report-into-youth-harm-online-released>
28. Inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in - NationBuilder, accessed on June 15, 2026,
https://assets.nationbuilder.com/actnz/pages/30993/attachments/original/1765330956/Final_interim_report_%28Inquiry_into_the_harm_young_New_Zealanders_encounter_online_and_the_roles_that_Government_business_and_society_should_play_in.pdf?1765330956
29. Final report on harm young New Zealanders encounter online ..., accessed on June 15, 2026,
<https://vine.org.nz/news/final-report-on-harm-young-new-zealanders-encounter-online-released-related-news-and-research>
30. Draft report (Inquiry into the harm young New Zealanders encounter online, and the

roles that G.docx, accessed on June 15, 2026,

<https://selectcommittees.parliament.nz/download/SelectCommitteeReport/51deb7d3-6f4c-48bb-8a93-08de7a2437b3>

31. Catherine Wedd Explains Her Proposal To Ban Social Media For Under-16s - YouTube, accessed on June 15, 2026,
<https://www.youtube.com/watch?v=YR9wSrvW8qk>
32. Should Social Media be Banned? Online Child Safety in NZ - UNICEF New Zealand, accessed on June 15, 2026,
<https://www.unicef.org.nz/stories/should-social-media-be-banned-for-children>