MEMO *Published March 13, 2026 · 9 minute read*

How to Protect Kids Online: The Building Blocks of Online Safety Policy

Ruth Whittaker

By age 13, 81% of children have their own smart device, and 95% of teens between the ages of 13-17 have their own smartphone. [1] Parenting in today's world is not for the faint of heart. Nearly two-thirds of parents say raising kids is harder than they ever expected, a sentiment few would find surprising. [2] Beyond the timeless challenges of getting kids to eat their vegetables, sleep enough, and keep up with homework, modern parents are now responsible for something entirely new: shepherding their children through a digital landscape that changes so quickly that even experts struggle to keep up.

Policymakers are responding with new proposals to protect children online, but the challenge is finding strong enough guardrails that protect children without undermining privacy, free expression, or access to information for kids and adults alike. Below, we unpack how policymakers can protect kids online without undermining the benefits that digital tools provide for learning, connection, and independence. We outline a balanced framework that takes a risk-based approach, accounts for the diverse needs of children and families, and establishes strong default protections that can be customized as users and technology evolve.

Current Situation & Why Balance Matters

A growing body of research shows the real and lasting downsides of phones and screens. The American College of Pediatricians warned that "excessive exposure to screens, [...] especially at young ages, is associated with lower academic performance, sleep disturbances, obesity, attention deficit, increased aggression, lower self-esteem, depression, and increased rates of high-risk behaviors." [3] Screen addiction is a worry for every parent, and it is so prevalent that there are even in-patient treatment facilities for adolescents. [4]

There are also upsides. Smart devices are enormously powerful tools that offer real benefits for learning, independence, and connection. They can support busy families with educational tools and give kids a reliable way to stay in touch in emergencies. For many teens, online communities and social media also provide space for creativity, self-expression, and support during difficult times. Artificial intelligence can provide personalized tutors to students, expanding learning opportunities and empowering kids with individualized support.

Policy proposals have responded to online risks in a wide variety of ways. Australia last year passed a law "restricting all users under 16 from holding accounts on major platforms including TikTok, Snapchat, YouTube, Reddit, Instagram, Facebook, Kick, Twitch, Threads and X." [5] The Australian law has attracted interest from lawmakers across the world. In the United States, the House Energy & Commerce Committee recently considered 18 bills ranging from wholesale bans on social media to updates to children's privacy rules and requirements that platforms redesign or block certain features for kids. [6]

Is it possible for a balanced approach to work for parents and kids, and if so, what would it look like? All kids are different, all families are different, and the proliferation of new platforms and technologies present unique challenges. A balanced approach will have to be layered, flexible, and adaptable.

At minimum, efforts to protect kids online should:

1. Take a risk-based approach that maximizes protection for kids and minimizes friction for adults.
2. Recognize every family has different needs.
3. Combine strong default protections with flexibility for parents to customize rules that fit their family.

Risk-Based Approach

Broad rules that require *all* online spaces to be kid-appropriate risk limiting internet access for everyone. Treating child users differently also means platforms must reliably distinguish children from adults which, in practice, often requires more data collection and adds inconveniences (or "friction") for adult users. Overly sweeping mandates could burden free speech, slow innovation, disrupt everyday online services, and handicap the next generation by stunting their digital and AI literacy.

Instead, policymakers should take a *risk-based approach*—maximizing protection for kids while minimizing friction for adult users. That means tailoring rules based on both the *level of risk* a platform poses and how *likely* children are to use it. The image below shows how these axes work.

[graphic]

Online experiences in the bottom left corner are easiest to address. Niche news sites and workplace productivity tools probably don't need to create alternative child-safe environments or verify every user's age, since they pose little risk and are unlikely to be accessed by kids in the first place.

Similarly, requiring platforms in the bottom right quadrant (easily accessed but not risky) to adopt heightened protections or build child-specific experiences would simply add friction for all users without meaningfully increasing safety. Do we really need to upload a driver's license to access a weather app?

Apps and platforms in the top left quadrant must have protections for kids, but they are likely already covered by other regulations that make it difficult or unlikely for kids to access them. For example, online gambling platforms are prohibited by state laws from allowing minors. Stock trading apps are already required to collect identity information under Anti-Money Laundering and Know Your Customer laws and are prohibited from entering into financial contracts with minors.

Policymakers should focus on the top right quadrant—experiences that are easily accessible and pose more risk—when designing heightened, child-specific requirements.

But policymakers should also remember that the level of risk within that quadrant can vary. Nearly all social media sites would likely fall into this category of easy to access, riskier platforms, but not all social media sites are created equal. Chatroulette, which randomly matches users for live conversations, or Kik, which enables anonymous messaging, pose more risk to kids than sites where users have more control over who they interact with, like Instagram or TikTok.

The same can be said for artificial intelligence. Some applications of AI, like character-based chatbots, may fall into the high risk/highly likely to be accessed quadrant, but policy responses to those applications should be targeted. Regulating the technology rather than the use risks undermining the benefits for kids and parents.

To be sure, policymakers alone can't always determine the risks of every technology, platform, or website. This approach requires coordination with parents, researchers, civil society, and the tech industry to make sure risks are properly measured—and that the policies that address them are actually effective. The benefit of a risk-based approach is that it produces targeted regulations that respond to specific concerns and minimizes unintended consequences.

Recognize Diverse Needs

Every kid is different. A 16-year-old will navigate the internet differently than a 13-year-old. Even within the same age group, children have different interests, different levels of maturity, and very different relationships with the adults in their lives. Policies that treat everyone under 13 or 18 as a monolith risk compounding harm for already vulnerable kids —or letting others fall through the cracks.

A one-size-fits-all approach also assumes every child has the same level of adult support and supervision. But kids' relationships with parents and guardians vary widely. Proposals that give parents total veto power over online experiences or blanket access to kids' personal data could put some children at greater risk, including those experiencing abuse or those in households that don't support their sexuality or gender identity.

And not every parent has the time, resources, or technical skills to manage a maze of privacy settings or complicated age-verification systems. Kids shouldn't get a worse version of the internet simply because their parents aren't tech-savvy. Similarly, families who are hesitant to provide sensitive personal information—especially amid heightened fears of immigration enforcement—shouldn't be effectively cut off from the modern digital world.

Instead, policymakers should build flexibility into kids' safety frameworks.

That flexibility should recognize multiple developmental stages within a child's online life. Older teens, in particular, deserve increasing autonomy online as they approach adulthood. In most states, a 16-year-old can drive a car, hold a job, and even fly a plane. [7] It makes little sense to deny them meaningful control over their privacy, settings, and digital interactions.

A strong safety framework should also protect children without assuming every family looks the same. Ensuring access to online spaces—even for kids without active parental supervision—helps prevent policies from compounding harm for the very children they are meant to protect.

Create Strong Baseline Protections, But Allow Customization

The most effective way to address online risk is to require strong safety and privacy protections by default and allow families to adjust those settings over time. Safety and privacy by design ensures every child starts with a meaningful level of protection, without requiring parents to monitor every app, platform, or technology their child uses.

Defaults matter. Establishing strong baseline protections reduces the burden on parents and gives kids room to explore online without waiting for case-by-case permission. At the same time, allowing customization—especially as children get older—acknowledges differences in maturity, independence, and family expectations.

This approach also aligns with a risk-based framework discussed above. As online experiences move up the risk axis, default protections should increase. So too should the friction required to remove them.

For example, consider an online gaming platform with child-friendly games that includes in-game purchases and direct messaging with other players. Baseline protections enabled by default could disable messaging with unknown adults, limit contact to approved friends, and place guardrails around in-app purchases. Younger users might need parental approval to adjust those settings, while older teens could be permitted to modify some controls independently. That structure guarantees a base level of protection while recognizing that a 17-year-old's expectations of privacy and autonomy differ from those of a 10-year-old.

Higher-risk platforms warrant stronger defaults. Alcohol delivery services, for example, should require automatic ID verification before granting access to age-restricted products. That added friction for adult users mirrors what we expect in the offline world and is appropriately calibrated to the risk for minors.

But allowing parents to adjust those default settings to fit their families' needs is also important. A risk-based framework should allow parents and kids to tailor the level of protection to each child's unique needs. Parents should also be empowered to determine how much oversight they need over their kids' online experiences—while being assured that their kids will be protected no matter what.

Online safety is a shared responsibility among users, parents, and platforms. Policymakers should establish baseline safety requirements for all platforms, calibrate those requirements to their level of risk, and empower families and teens to shape their digital experiences over time.

ENDNOTES

[1] "Screen Time Statistics Reveal How Parents Use Screens as Babysitters, Educators, and Entertainment Tools". Ann & Robert H. Lurie Children's Hospital of Chicago, 30 Oct. 2025. https://www.luriechildrens.org/en/blog/screen-time-2025/#:~:text=The%20majority%20(81%25)%20of,age%20to%20start%20screen%20time. Accessed 6 Mar. 2026; Sidoti, Olivia, et al. "Teens and Internet, Device Access Fact Sheet". Pew Research Center, 10 July 2025. http://pewresearch.org/internet/fact-sheet/teens-and-internet-device-access-fact-sheet/. Accessed 6 Mar. 2026.

[2] Minkin, Rachel and Juliana Menasce Horowitz. "Parenting in America Today". Pew Research Center, 24 Jan. 2023. https://www.pewresearch.org/social-trends/2023/01/24/parenting-in-america-today/. Accessed 6 Mar. 2026.

[3] "Media Use And Screen Time – Its Impact On Children, Adolescents, And Families". American College of Pediatricians, May 2020. https://acpeds.org/media-use-and-screen-time-its-impact-on-children-adolescents-and-families/. Accessed 6 Mar. 2026.

[4] Mayer, Beth Ann. "7 Signs Your Kid Has Screen Addiction and What To Do About It". *Parents,* 13 Nov. 2025. https://www.parents.com/signs-of-screen-addiction-in-kids-11848694. Accessed 6 Mar. 2026.

[5] "What is Australia's under-16 social media ban? The world-first law explained". University of Sydney, 5 Dec. 2025. https://www.sydney.edu.au/news-opinion/news/2025/12/05/what-is-australias-under-16-social-media-ban-the-world-first-law-explained.html. Accessed 6 Mar. 2026.

6. "CMT Subcommittee Forwards Kids Internet and Digital Safety Bills to Full Committee", Press Release, *House Energy & Commerce Committee,* 11 Dec. 2025. https://energycommerce.house.gov/posts/cmt-subcommittee-forwards-kids-internet-and-digital-safety-bills-to-full-committee. Accessed 6 Mar. 2026.

7. "Driving Age by State: Permit & License Ages (2026 Guide)". Thompson Law Injury Lawyers, https://1800lionlaw.com/driving-age-by-state/ ; "Child Labor Laws by State + Federal (2025)". Workforce.com, 27 Dec. 2024, https://workforce.com/news/minor-labor-laws-by-state#Wisconsin. Accessed 6 Mar. 2026; "Student Pilot's Certification Requirements". Federal Aviation Administration, 12 Nov. 2022. https://www.faa.gov/pilots/become/student_cert. Accessed 6 Mar. 2026.