Practical Protection: The EU Kids Act

Google's High-Level Policy Positions on the Keeping Internet Digital Spaces Accountable and Trustworthy Act (EU Kids Act; COM(2026) 681 final)

Overview

For young people across Europe, the digital world is an essential space for education, creativity, and connection. Research from The Future Report 2026 shows that European teenagers actively use digital tools and AI every day to master difficult school subjects, explore new passions, and stay informed about the world around them, while also demonstrating strong critical thinking and personal agency in managing their online habits.

At Google, keeping young people safe online does not start with new legislation. Across YouTube, Google Play, Gemini, and our wider product suite, we continuously invest in age-appropriate defaults, age assurance, safety filters, and practical family tools.

Our guiding view is simple: **Europe should protect children in the digital world, not from the digital world.** We strongly share the European Commission's ambition in the proposed *Keeping Internet Digital Spaces Accountable and Trustworthy Act* (the EU Kids Act) to establish a single, harmonised European rulebook built on robust safety-by-design standards.

While the draft Act takes welcome steps toward a feature-based and graduated framework, several provisions as currently written risk undermining the very protections they aim to strengthen; disabling by default safety-enhancing implicit signals in personalised recommendations, pushing open-web users behind identity walls, limiting access to educational and informational tools regardless of their actual risk for minors, including cutting off teens from long-form videos and music, blocking the use of tools that detect if a user is a child, and leaving gaps for fragmented national bans. With targeted, practical adjustments, EU co-legislators can deliver a framework that is clear, privacy-preserving, enhances safety, and is genuinely effective for families across all 27 Member States.

1. Core Principles for Effective Online Child Safety

Smart child-safety legislation should build on Europe's existing digital rulebook, including the Digital Services Act (DSA), the Audiovisual Media Services Directive (AVMSD), the GDPR, and the EU AI Act, rather than creating overlapping obligations or rigid, one-size-fits-all bans. Five core principles guide Google's engagement on the EU Kids Act:

- **Protect children in the digital world, not from it:** Young people rely on digital tools to learn, create, explore, and connect. Rules should target real harms while preserving access to education, culture, and reliable information.
- **Same feature, same rules:** Regulation should address specific risky features through proportionate safeguards tailored to their risks—such as unmoderated stranger contact or coercive in-game spending—consistently across every service that offers them, rather than exempting identical features based on business model. At the same time, it should recognise that access to movies, documentaries, music and other forms of content should be treated in the same way as exactly the same forms of content are treated on equivalent services, such as streaming platforms and music streaming services.

- **Privacy by design and an open web:** Age-assurance rules must remain risk-based, flexible, proportionate and privacy-preserving, never forcing everyday adults to undergo strict age verification checks simply to access news, or watch an educational video without an account and/or when platforms already have reliable indications that they are an adult.
- **Empower parents and respect teens' growing maturity:** Parents know their children best. The law should provide strong protective defaults that guardians can tailor to their family, while granting older teens graduated autonomy as they prepare for adulthood.
- **One unified European rulebook:** To safeguard the Digital Single Market and avoid 27 conflicting national laws, the Act must deliver true EU-wide harmonisation paired with realistic implementation timelines and proportionate compliance and oversight rules that build on—rather than duplicate—existing DSA frameworks.

2. Five Practical Refinements for a More Effective and Pragmatic EU Kids Act

The table below summarises the five core pillars where targeted refinements would align the EU Kids Act with real-world technology, family life, and Single Market principle.

Strategic Pillar	Core Challenge in the Draft Act	Google's Proposed Solution
Fair Scope & Level Playing Field	Lack of equal treatment between video-sharing platforms and streaming/audio competitors which operate with identical features such as personalised recommendations and autoplay. Applies blanket feature restrictions to video-sharing platforms without excluding long-form video, movies, documentaries, music and other content where there should be parity with other service types. Sweeps in everyday utilities and very low risk single-player games.	Apply equivalent rules to equivalent features or exempt long-form media and music across all such services. Add a horizontal main purpose test or ancillary-features carve-out and focus gaming rules on stranger chat and paid loot boxes.
Personalisation & Healthy Habits	Treats personalised recommender systems as inherently harmful to minors and prohibits safety-enhancing implicit signals for U15s; imposes rigid 1-hour caps, blackouts, and mandatory autoplay interruptions on music, learning content and family film viewing.	Restore U18 minor and guardian choice over personalised recommendations. Recognise the value of implicit signals for minors of all ages to optimise for high quality content, prevent “rabbit-holes” and disperse low quality content. Prioritize age appropriate safety rules. Exclude long form content and music for indiscriminate autoplay interruptions. Make daily time limits and sleep/school reminders guardian-configurable - to set defaults and lift limits as required.
Age Assurance & Open Web	Mandates reliance on unready national wallets and bans certified wallets offered by the same provider as the relying party; converts advisory app ratings into hard blocks on browsers and dictionaries; misapplies OS requirements; forces signed-out web users through age checks; weakens parental-control security; blocks the use of existing age tools. Restrictive safety by design obligations (such as tracking cumulative watch-time caps or enforcing 22:00–08:00 sleep curfews) extend to signed-out users, meaning that signed-out users are effectively treated like a minor, when signed-out use of YouTube has significant use cases, such as via the TV or News Publisher websites who choose to host videos on YT and embed the content in their own websites.	Adopt a proportionate two-step age-assurance model (age-estimation signals first, reserving verification—without exclusive EU wallet mandates—for inconclusive cases); on guardian-managed accounts, let a guardian's age declaration replace separate age assurance of the child (preserving practical guardian verification where national parental attestations are unavailable); remove OS age-sharing mandates (or limit OS strictly to neutral pass-through infrastructure); scope account rules to signed-in sessions; and allow national and private wallets for the trust lists; delete parental-control interoperability mandates;keep ratings advisory with developer in-app responsibility for statutory age limits and a ‘safe harbour’. To ensure equitable access to online information and services, requirements must remain flexible to accommodate legitimate uses of signed-out mode.
AI & Learning Tools	Fails to focus on mitigating priority risks; captures everyday productivity tools, navigation assistants, and school-licensed software; breaks multi-day tutoring memory, exam study, and accessibility tools.	Narrow Companion AI to systems replacing human companionship; scope general conversational chatbots to multi-session systems while excluding task-oriented tools (such as information retrieval, navigation, drafting, and media tools) and systems with built-in safety guardrails against companionlike or similar behavior; carve out B2B, and school-licensed software; allow user-controlled memory, single-task sensors, and AI Act/DSA alignment.
EU Harmonisation & Timelines	Leaves backdoors for diverging national age limits and breaks DSA alignment;imposes pre-application compliance-plan audits, duplicate VLOP supervisory fees sets unrealistic 30-day VLOP plan and 6-month transition deadlines.	Codify maximum harmonisation and DSA Art. 28(1) alignment; extend VLOP plans to 4 months without pre-application audits, relying on existing DSA cycles; integrate DSA audits. Add a binding maximum-harmonisation clause barring conflicting national age limits or safety-by-design mandates; exempt VLOPs already paying DSA supervisory fees from duplicate charges; and set a 24-month general implementation period.

3. Key Challenges and Practical Solutions

Although the proposal sets the right overarching direction, five structural challenges risk creating unintended consequences for young people, families, and everyday internet users. Addressing these five areas would make the EU Kids Act both durable and more effective at protecting minors.

Google's view is that a tiered access regime for the draft Act risks diverting from actual risk, and from the opportunity of creating age appropriate spaces online. Blanket restrictions on minors' accounts risk incentivising young people to borrow adult logins or migrate to less safe services, moving away from the protections that accounts make possible. Also, blanket interventions raise concerns with fundamental rights to receive and impart information and to privacy, because in practice compliance would require age checks for every user, adults included.

Instead, strong, harmonised safety-by-design requirements give minors crucial protection for their privacy, safety and security on in-scope services. The draft Act should expressly stipulate that, and prevent fragmentation through uncoordinated restrictions to minors' access to those safe-by-design services, stricter age limits or other requirements.

3.1 Ensure a Fair, Feature-Based Scope Across Digital Services

The EU Kids Act should treat comparable risks consistently across the market rather than penalising specific platforms while sparing identical experiences elsewhere. Today, the draft imposes rigid 1-hour daily caps, overnight curfews, and continuous-play bans on video-sharing platforms like YouTube, while exempting video-on-demand, podcasting and audio streaming services in respect of identical or substantively similar content such as podcasts, movies, music and other long-form content. Under that split, a teenager watching a two-hour educational documentary or listening to a music album on YouTube would be cut off by law, whereas the exact same documentary or album on a streaming competitor would face no restrictions.

Scope overreach compounds this across three related fronts. First, standard content or personalised recommendations and continuous play trigger sweeping account lockouts for under-15s across entire video platforms, while open-ended delegated powers let the Commission add new access-ban triggers later without full legislative scrutiny. Second, unlike the DSA and the AVMSD, the draft lacks a horizontal primary-purpose test—meaning light interactive touches such as restaurant reviews in Google Maps, shared albums in Google Photos risk subjecting everyday utilities to disproportionate restrictions which were never intended to apply to the underlying services. Third, broad gaming definitions sweep in harmless single-player puzzles, casual mini-games, and educational games with no chat or purchases, while risking confusion between coercive paid loot boxes and ordinary earned gameplay badges. We recommend:

- **Align rules to equivalent features or exempt music and long-form media:** Apply comparable safety-by-design rules to equivalent features on streaming services, or exclude long-form video (such as documentaries, films, and lessons), music, and podcasts from caps, curfews, and continuous-play bans.
- **Target real risks rather than standard infrastructure:** If the delayed access regime is maintained, remove standard recommendations and continuous play as account-ban triggers, delete or narrow open-ended delegated acts, codify a horizontal main purpose/ ancillary-features test, and limit gaming rules on features posing material risk (like open stranger chat and paid variable rewards).

3.2 Allow Safety-Enhancing Personalisation and Support Flexible Online Habits

Responsibly designed recommender systems use personalisation to deliver safer, more appropriate experiences based on user age and developmental stage. They also limit user exposure to content that is not age appropriate, or off-putting, irrelevant, or not enjoyable. The Kids Act should preserve a risk-based approach that enables the use of responsible personalised recommendations by maintaining implicit signals as a vital component of minor protection.

The most obvious benefit of personalised recommender systems is structuring and prioritizing the near-limitless volume of online information to make it easier and faster for users to find what's most helpful and meets their needs. This is a universal practice adopted across almost all online services, including media, video, shopping, and music streaming services. Personalisation delivers additional benefits to young people in many ways, in particular by mitigating repeated exposure to certain types of content, including content that is potentially harmful in repetition; supporting learning; connecting to content that deepens their existing interests and perspectives, mainstream and otherwise; and broadening their interests beyond their narrow starting point. Whilst poorly designed recommendation systems may be designed to extend engagement, responsibly designed systems can optimise for these benefits.

Rather than enhancing safety, turning off implicit signals by default would make it more difficult to find age-appropriate educational material, lead minors into narrow content loops, and ultimately leave young users on these platforms not just with a less enriching, but also a less safe experience. This would result in severe, unintended consequences for platforms that have designed their recommender systems responsibly.

Blunt usage cutoffs create similar friction for real families. Non-overridable 1-hour daily caps, fixed 22:00–08:00 and school-hour blackouts, mandatory pop-up interruptions, and blanket autoplay bans disrupt recorded lectures, music albums, podcasts, Friday-night family films, and extended homework. Leading authorities—including the Council of Europe, the UN Committee on the Rights of the Child, the European Academy of Paediatrics, and EU Kids Online researchers—emphasise graduated autonomy over rigid bans that only encourage parents to hand children their own adult logins, stripping away youth safeguards entirely. For the Kids Act, we recommend to:

- **Protect responsible personalisation with user choice:** On video-sharing platforms, replace the default-off mandate on implicit engagement signals with informed choice (permitting default-on recommendations with easy opt-out controls) for minors aged 15+ and guardians for minors under 15, alongside easy feed-reset tools and DSA non-profiled options; in dedicated under-13 guardian-controlled VSP experiences, allow guardians to expressly enable functional personalisation, non-profiling recommendations; replace rigid explicit-over-implicit signal hierarchies with prioritising age-appropriate content, and proportionate safeguards against repeated harmful exposure ("rabbit holes"); and permit cross-service data based on valid, specific consent (or narrow purpose-limited grounds under GDPR.
- **Carve out long-form and music content from control tools and parental flexibility:** Exclude long form, music and podcast content from autoplay and infinite scroll interruptions, and allow guardians controls to adjust daily limits, bedtime reminders, and study schedules.

3.3 Build Privacy-Preserving Age Assurance and Protect the Open Web

Effective age assurance must reflect how digital devices and families actually work without erecting identity walls across the open internet. Requiring platforms to rely on certified EU age-verification solutions from day one risks excluding millions of Europeans before national eIDAS wallet infrastructure operates across all 27 Member States—particularly disadvantaged teens and individuals without qualifying IDs, bank accounts, or compatible devices.

Furthermore, "independent third-party" corporate-separation rules exclude certified commercial and ecosystem wallets that are issued by the same provider as the relying party and that invest heavily in hardware-isolated security, regardless of existing safeguards. Simultaneously, while we support zero-knowledge proofs (ZKPs) for cryptographic verifiable credentials, they are technically incompatible with non-cryptographic assurance models. Moreover, blanket prohibitions on evaluating internal account or cross-service signals effectively ban privacy-preserving age estimation, and prevent parents from sharing their child's age with platforms These restrictions blind machine-learning tools that help distinguish shared family households, such as when a parent streams children's cartoons on a living-room smart TV using an established adult account while managing adult email and banking services elsewhere.

The draft also **misaligns operating system and app-store duties**. Modern privacy-preserving identity separates a digital wallet from the system carrying it. An operating system (such as iOS, Windows, or the Android Open Source Project) runs a device's screen and apps and, by deliberate privacy design, does not know who the user is; instead, it acts as a neutral, secure "pipe" (via standardized interfaces like the W3C Digital Credentials API and Android Credential Manager API) connecting local wallets to websites and apps, while family supervision and age-bracket sharing reside at the account and app-distribution layer.. Meanwhile, turning advisory app-store ratings (like PEGI, USK, and IARC) into hard technical download blocks would lock a 15-year-old out of a standard web browser, news app, or dictionary for schoolwork, override parental approvals inside family supervision tools, and ignore pre-installed or sideloaded apps. At the same time, mandating interoperability between proprietary family tools like Google Family Link and unvetted third-party apps risks exposing sensitive child activity logs and weakening safety filters.

Equally concerning are the proposal's **effects on signed-out browsing and teen accounts**. Treating every signed-out visitor as an unverified minor until adult status is proven—while simultaneously prohibiting persistent tokens—would force commuters, journalists, or someone looking for a "how-to" video to fix the Wi-Fi to log in and prove their identity just to read news, find directions, or view full search results. That identity wall directly undermines privacy and the right to receive and impart information under Article 11 of the EU Charter of Fundamental Rights. As an already restricted, view-only experience with universal baseline protections (such as blocking age-restricted content), YouTube signed-out mode serves an important adult user base across the EU and supports the broader media ecosystem. Scoping it into the full breadth of Chapter III Safety-by-Design requirements risks turning signed-out mode into a *de facto* under-13 experience unless users prove they are adults, introducing unnecessary friction for news publishers who host and embed YouTube videos on their own websites. Separately, overly rigid "mini-account" restrictions and unworkable guardian-verification burdens risk undermining the realistic middle ground families need: balanced, supervised view-only accounts for younger teens with clear parental oversight.

Finally, to ensure equitable access to online information and services, **age-assurance frameworks** must remain flexible and accommodate individuals who cannot obtain or utilise a digital wallet. Temporarily displaced persons seeking refuge in the EU may lack the formal legal status or documentation required to generate digital wallets for themselves or their dependents, relying instead on signed-out access or supervised YouTube experiences; strict wallet mandates would disproportionately disadvantage an already marginalised group. Older adults likewise require flexible, accessible alternatives to prove they are over 15 without being forced to rely exclusively on the EU Digital Identity Wallet. Similarly, children in shared custody, foster care, or lower-income households may not have a single, cooperative, or digitally capable adult available to verify their identity or manage linked accounts—meaning mandatory parental or wallet-based gating would effectively disenfranchise these young people from vital educational content, tutorials, news, and digital literacy tools.

To resolve these gaps coherently, co-legislators should anchor age assurance in a proportionate, privacy-preserving architecture across every layer:

- **Adopt a two-step targeted verification model:** Rely first on low-friction behavioural signals, ring-fenced first-party cross-service safety signals (strictly banned from advertising), and parent-provided age signals (removing the ban on parents informing platforms of their child's age), reserving hard cryptographic wallet checks for instances where the initial filter cannot reliably establish eligibility. End exclusive reliance on EU Age Verification Wallets so less-intrusive alternatives remain permanently valid, remove 'independent third-party barriers so any certified wallet meeting objective security and privacy standards qualifies for the EU Trust List, and confine mandatory ZKPs to cryptographic verifiable credentials while preserving privacy-preserving selective disclosure (cryptographic binary "yes/no" tokens) for routine threshold checks.
- **Assign clear layer roles, keep ratings advisory, and preserve open-web access:** Keep operating systems as neutral conduits maintaining open, standardized pipes (such as Credential Manager and W3C Digital Credentials APIs) for wallets, permit user-consented age signals and parental consent flags at the account and app-store layer, and leave primary legal liability with downstream apps and sites. Keep independent app-store ratings advisory on signed-in store accounts with guardian override controls, keep statutory age-gating responsibility in-app with developers and provide a safe harbor regime, allow view-only 13–14 accounts, guardian-managed child accounts, and 15+ upload visibility controls, delete risky parental-control interoperability mandates, and scope Chapter III safety-by-design defaults to authenticated accounts so signed-out open-web access remains protected.

3.4 Focus AI Guardrails on Emotional Risks While Protecting Education

Generative AI gives students powerful support for personalised tutoring, research, and future workplace skills, yet the draft's AI rules sweep far beyond addressing priority risks, such as unhealthy emotional attachments, mental health concerns, and inappropriate content. Defining conversational chatbots broadly while exempting only tools strictly "limited to" a narrow task risks pulling navigation helpers, and video-summarisation tools into rules written to address AI tools designed to simulate relationships. Failing to explicitly exclude school-licensed and B2B software such as Google Workspace for Education —already governed by teachers and school administrators— risks cutting access to educational tools that can build digital literacy and future employment skills.

Strict chatbot defaults would also harm learning and accessibility in everyday use. A single statutory 22:00 blackout cannot be harmonised across Europe's diverse family schedules and bedtimes, and cuts off pupils revising late for exams or seeking crisis helpline guidance; wiping memory after every session forces an AI tutor to forget progress on a multi-day homework project; rigid default-off restrictions on camera, microphone, and location inputs break textbook translation and real-time visual assistance relied upon by users with disabilities; and vague pre-market testing rules duplicate obligations already under the EU AI Act and the DSA.

- **Require risk-based safety-by-design and carve out educational, informational, and B2B tools:** Anchor safety-by-design in non-negotiable guardrails for minors—prohibiting sentience claims and romantic/emotional simulation, mandating active clinical crisis redirection for self-harm, and banning variable rewards and unsolicited re-engagement nudges—while limiting Companion AI obligations to systems providing sustained, personalised emotional or social relationship simulation. Broaden exemptions for General Conversational Chatbots to tools that "primarily relate to" specialised tasks—such as navigation, information retrieval, collaborative drafting, and media/video assistance—as well as AI systems with built-in design safeguards against companion personas, simulated intimacy, or self-harm. Additionally, exclude services accessed via school-provisioned educational accounts and B2B services.
- **Preserve study continuity, accessibility, and regulatory alignment:** Replace fixed curfews with guardian-configurable reminders, allow user-controlled cross-session memory with clear deletion tools, permit user-initiated single-task sensor access, and align risk evaluations with existing DSA duties.

3.5 Guarantee One European Rulebook and Realistic Implementation Timelines

Leaving room for 27 diverging national age laws undermines families and fragments the Digital Single Market. Although the Act is built on Article 114 TFEU, its recitals still permit Member States to maintain higher national age limits for specific content categories and state that compliance does not automatically satisfy DSA Article 28(1), leaving a backdoor for conflicting national rules. At the same time, giving existing Very Large Online Platforms just 30 days to submit pre-application compliance plans (within just 30 days for existing VLOPs), charging duplicate supervisory fees alongside the DSA, and setting a 6-month general transition before key delegated acts are ready asks engineering teams to deliver complex safety pipelines on impossible schedules while duplicating annual DSA risk assessments and audits.

- **Lock in maximum harmonisation:** Add a binding maximum-harmonisation clause barring conflicting national age limits or safety-by-design mandates, clarify that complying with the EU Kids Act satisfies DSA Article 28(1), and maintain 12-month TRIS standstills against diverging national bills, including those seeking modifications to laws originally notified under TRIS prior to the standstill period.
- **Align timelines and audits with real-world readiness:** Reframe Article 5 filings as preliminary compliance plans due 4 months after general application—removing mandatory pre-application audits and allowing providers to rely on existing DSA risk assessments and compliance documentation—set a 24-month general implementation period (with immediate empowerment to adopt technical acts in advance), and exempt VLOPs already paying DSA supervisory fees from duplicate charges.

Together, these five adjustments preserve the Commission's safety ambitions while making the framework workable across platforms, families, and national borders.

Conclusion

Protecting children online does not require dismantling the open internet, infringing on minors' right to information, or asking every European citizen for an ID card at the digital door. By pairing a level playing field across services with risk-based requirements, safety-enhancing personalisation, a practical waterfall approach to age assurance, respect for parental discretion and teen maturity, and a single harmonised European rulebook, co-legislators can make the EU Kids Act both effective and enduring.

Google welcomes the opportunity to work constructively with the European Parliament, the Council, the European Commission, civil society, and industry partners throughout the legislative process to ensure Europe's digital spaces remain safe, open, and empowering for current and future generations.