



Policy Enhancement
Recommendations Brief

Child Online Safety Suggestions

Autumn 2026

Protecting children starts with understanding their digital lives

Sources: European Commission consultation with children aged 12–17 across all 27 Member States; BCG; Pew Research Center

72%

of children have encountered at least one cyberthreat

11%

of children would tell no one if they were being cyberbullied

24%

of children in the EU say cyberbullying happened to them

39%

have seen it happen to someone else

57% do not know whether their school has any rules against bullying

43%

of children with a disability were cyberbullied, against 20% of others

40%

make new friends inside games and communicate with them there

Asked what would help, children named: easier reporting, follow-up on it, real enforcement of the rules, emotional support, openness, resilience.

EU Children's Participation Platform, November 2025

Countries are recognising the challenge and building the first layer

A child spends most of their free time in the digital space. Instagram, TikTok, Snapchat, Discord, Roblox, dozens of games. That is where they meet people, make friends, spend money and find things they get nowhere else. It is also where they are found by adults who are looking for them. It is also where adults can target them – sometimes for seemingly harmless contact, but potentially leading to grooming, scams, or involvement in illegal activities.

Countries are responding. In the EU, the DSA sets platform obligations to protect minors, supported by the European Commission's age-verification blueprint. Some countries have already begun introducing age restrictions on social media access.

We see this as the right first layer, which definitely plays its role. The challenge is relying on it alone, as limited restrictions without broader safeguards may reduce some risks while creating new ones.

The gate is bypassed because the child wants to bypass it

When Australia introduced an age ban for social media, over 4 million accounts were reportedly deleted from the platforms. At the same time, no decrease in cyberthreats to children was reported. Around 70% of children later responded that they continued using social media.

Children described how they get around the checks: they use someone else's data, switch accounts and devices, or ask an older sibling to pass the face scan for them. They share these methods with each other. They call the restrictions unfair.

Now, when something bad happens, the child has two reasons to stay silent: first, they need to admit that they broke the rules, and only then say that something bad has happened. The metrics may not capture such cases, creating a false sense of security until considerable damage is done.

Australia introduced a social media ban for under-16s on 10 December 2025 – the first of its kind globally. While millions of accounts have been removed, children are finding workarounds, with demand for VPN services reportedly skyrocketing. Similar patterns were seen in the UK following the introduction of age controls.

When I was bullied at school, it had a closing time. I went home, shut the door, and until morning it stopped. Today there is no such door.

Ignat Bobrovich, founder

They literally just asked me what my age was, and then, like, 'are you sure?' I just clicked 'yes I'm sure'

Boy, 14, Australia, after the ban

We do not build the fence higher. We remove the reason to climb it

Valvur connects the child, the parent, the school, the platform and the state into one loop. Openness and safe behaviour bring the child what they want, while risks along their path are caught at several points at once. This works today, not on a roadmap: the family application, the schools module, and on-device detection in chats with the Edge AI module.

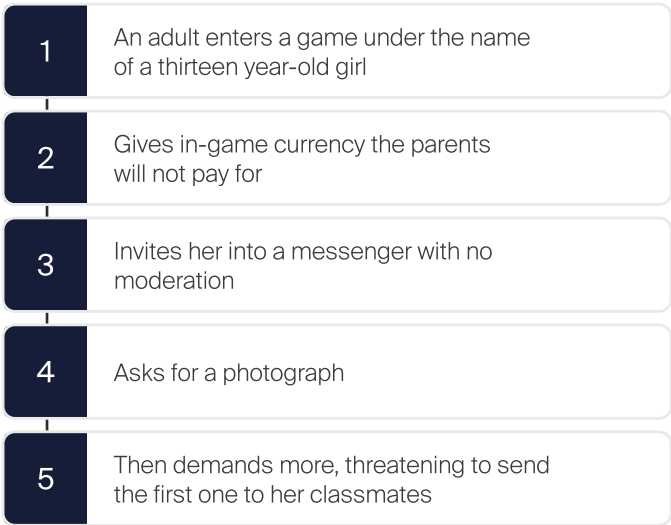
What children actually face online

Cybersecurity for a child no longer means protection from hacking. It means protection from cyberbullying, fraud, manipulation, sexual coercion, harmful content and hate speech, fake voices and videos, and people who hide who they really are. More than seventy per cent of children have already encountered at least one of these.

Type	Details
Contact and exploitation	Grooming under a false identity. Requests for a photograph, then for more. Sextortion. Fake voices and videos used to build trust or to threaten. Lawsuits over child sexual exploitation on Roblox · Bloomberg investigation, 2024
Peers	Cyberbullying that follows the child home. Humiliation in group chats. Being deliberately left out. Pressure that adults never see. 24% of children in the EU say it happened to them · 11% would tell no one · 43% among children with a disability, against 20% of others
Money	Scam messages. Gambling mechanics built into ordinary games. Casino-style games on platforms made for children. Spending that a parent never agreed to. Casino-style games circulate on child platforms such as Roblox
Influence	Propaganda and disinformation produced at scale for almost nothing. Bots in open comment sections. Radicalisation. Recruitment paid for in in-game currency. The Financial Times documented cases where errands paid in game currency ended in national-security charges
Data and AI	Personal data flowing into models owned outside the EU. A model that agrees with everything becoming the adult a child trusts most. Data harvested now to be decrypted later. The BBC reported AI companions developing sexual content with minors

The risks children face online go far beyond traditional cybersecurity. Across games, social platforms, messaging, and AI, they face exploitation, bullying, financial manipulation, harmful influence, and data risks – often across multiple platforms at once. Addressing them requires a broader strategy combining active protection, digital resilience and education, privacy by design, trusted identity, parental engagement, and timely intervention when serious risks emerge.

Real-life scenario: when online contact turns into blackmail



Social media may not appear in that chain. 40% of children make new friends in games; more than half keep their friendships there.

This scenario is more common than many realise, yet research suggests that only a small share of cases are reported. Often, incidents become visible only if serious harm has occurred – from financial loss and exploitation to severe psychological consequences.

One child. Many platforms and services. Countless potential threats.

Children face risks across seven key areas of their digital lives. Age-based social media restrictions address just one

Before contact, while the child can still recognise manipulation. At entry, when it is checked who is facing whom. At the reward, when in-game currency becomes leverage. At the move between platforms. At the point when material is obtained. At the blackmail. And after, when it has already happened and the child needs to tell an adult.

RISK		DESCRIPTION
1	Before contact – trust, resilience, motivation	Lack of trust between the child, parent and other stakeholders (e.g. teacher, law enforcement agency)
2	Entry – identity and age	Kids can fake their age to bypass age restrictions. Predators can pretend to be much younger to appear as peers
3	Reward – when in-game currency becomes leverage	Children want to buy in-game items, leaving them exposed to offers from strangers when parents do not want to provide the funds
4	Move between platforms	Communication and exposure are not limited to social media – children have many touchpoints with chats and information
5	Material obtained	In DMs or closed chat, the child is offered in-game currency in exchange for a photo or service. They agree. And they fall into the trap
6	Blackmail	Once they fall into such a trap, the risks escalate. More photos or services demanded until the situation becomes critical
7	After – reporting, response, help	It is crucial to provide an ecosystem that does not shame or restrict children who are in the trap, but encourages timely reporting

Protection beyond limitation

Valvur has a comprehensive set of technological solutions and uniquely crafted content that helps increase online safety for children and families, while also strengthening overall cyber resilience and improving national cybersecurity by protecting and educating the most vulnerable audience

MODULE	WHAT IT IS
Family ecosystem Standalone app for iOS and Android. Can be deployed with customisations and full white-label	Child app: cyber hygiene taught through a game, XP, and the proprietary KIBI universe of characters, carrying the storytelling and rewards (e.g. skins, unlocks, collaborations). A player profile that travels into games, services, internet cafés, and esports ecosystems. Parent app: digital parenting guidance, a specialist chat, and a disclose → task → reward loop that makes telling the parent the rewarding move
Solution for education Per school or per municipality; national programme ecosystem.. Can be deployed with customisations and full white-label	Cyberhygiene for pupils and teachers. A gamification layer that turns curriculum tasks into in-app content with rewards. Safe environments for a named school, including game chats. Individual programmes built around the KIBI world. Regular testing run by advanced models. A closed AI perimeter for staff and pupils. Cyberthreat analysis (including pentests) and cyber resilience training
Identity enabling ecosystem API into games, AI services and social networks with advanced SDK for consent and transactions management and beyond	Own KYC system operating on industry-leading technology, plus integrations with national checks – telecoms, banks, and eID. A knowledge bank protected by post-quantum encryption, with a zero-knowledge module that answers third-party requests with a yes or no and discloses nothing else. A rights engine for statutory age limits and closed systems such as schools. A permissions module within the parent app
Active conversational protection SaaS, or a licensed Edge AI module on the client's own infrastructure	Voice and text. Bullying, scams, abuse, grooming signals, and attempts to move a child onto another platform. Connects to Discord, Roblox, and comparable environments. Ties into the player profile, so behaviour in public spaces carries rewards and restrictions. Can run on devices, ensuring that message content never leaves the device
Data protection and AI sovereignty An ecosystem that can be deployed as SaaS or on-premises, with a white-label interface for mass adoption	Classifies, de-personalises and encrypts data before it reaches any model, with controls over how much is disclosed and parental settings above that. A dedicated access AI services with its own interface and ability to connect to any model. Interoperability and safe usage of the context between the apps and models
Local languages enabler Embedded in the modules of the ecosystem as well interoperable with external services and models	Children do not write in academic English, and detection systems trained only on English can miss them. Hence, we develop dedicated models for cyberthreat identification, trained to work efficiently across languages and slang. The models can be trained beyond the cyberthreat context and are interoperable with external services
Public-authority module Modules that can work stand-alone or be integrated with national systems	Reporting of attacks and violations to the police. Integration with national access and record systems. Monitoring of public digital spaces: banned gambling and illegal-service advertising, propaganda, bot detection in open comment sections, early detection of new scam patterns with mass alerting. National cyber-hygiene programmes
Financial rails SaaS, licensed module with white-label or simple integration	A child wallet for fiat and digital assets, with parental limits on transaction type and size. Bank integration. Seamless in-game payment within agreed parameters

We designed the system not to see more than it needs. Conversation analysis ensures full preservation of privacy. Zero-knowledge answers yes or no without disclosing the data behind it. Post-quantum encryption protects children's records against harvest now, decrypt later.

Let's collaborate to build stronger protection for children and families online

We have worked on identity in gaming since 2018 (initially with the Passport.GG concept) and collaborate with national partners in over 40 countries globally. We have completed a pilot with the Estonian Cybersecurity Competence Centre and are launching a new consortium project involving a law enforcement agency in the European Union.

We do not aim to replace existing solutions or regulation. We support their development and implementation by building trust between children, parents, and other stakeholders, strengthening digital resilience, and applying modern tools to evolving digital threats.

A conversation

Forty-five minutes to work out which of this you need. No commitment.

An expert group or committee

We are ready to contribute to expert and regulatory working groups with practical experience, data, and insights from gaming, esports, digital identity, and child online safety.

A pilot

One country, one municipality, a limited group, one school, metrics agreed in advance. The family ecosystem and the schools module are pilot-ready today.

Our perspective helps show how children actually interact, spend, and move across digital platforms, bringing practical insights that can help identify gaps and turn regulation into effective real-world safeguards.

Frontier innovations

Our focus is not only on responding to today's risks, but anticipating what comes next. We develop innovative tools leveraging AI, zero-knowledge proofs (ZKP), post-quantum cryptography (PQC), and blockchain to stay ahead of rapidly evolving digital threats. We offer technical integration with the blueprint, a joint project, white-label deployments.

Valvur Cybersecurity | Tallinn, Estonia

tere@valvur.ai

