Children's Coalition for Online Safety

Statement on the UK Government's *Growing up in the online world* consultation

As organisations working with and for children, alongside experts in online safety and the digital world, we welcome the Government's renewed focus on improving children's lives by prioritising their safety and wellbeing online.

However, delivering real protection and positive outcomes for children means tackling systemic risks, not leaving parents and children to protect themselves. It also means making sure children, in all their diversity, are genuinely included and considered when we design and build the online world.

Tech companies must be held accountable for unsafe designs, harmful features and weak safeguards. Just as we would expect from any business offering products and services offline, they must prove their services are safe and appropriate for children. With strong regulation and evidence-based interventions, the Government can make the digital world a space where children can participate safely, with their wellbeing supported, but it must address the root causes of harm.

As individual organisations, many of us have submitted detailed responses to the Government's consultation to outline how the online world can be transformed for children.

As a coalition, we call on the Government to take four key actions to strengthen online safety and wellbeing for children:

1. **Make online experiences suitable for different ages by mandating clear, child-friendly principles**

We must see a risk-based, graduated approach where children's online experiences and protections evolve as they grow. What they can access should reflect both their level of maturity and the risks involved. Age limits should be applied where appropriate, but meaningful protection comes from managing access based on both age and risk across the entire digital environment - not just social media, but also AI chatbots, connected toys, educational technologies and gaming.

To make this approach work in practice, we propose a principles-based framework supported by strong, enforceable regulation. Tech companies should follow risk-based age limits, with meaningful consequences if they fall short - these must include business disruption measures and senior management accountability. Key principles should include:

- Reliable and privacy-preserving age verification: Companies must use proportionate, privacy-preserving methods to assess age and gate high-risk features in full compliance with UK GDPR and the Age-Appropriate Design Code, with robust enforcement by both the ICO and Ofcom.
- Graduated experiences: Children's access to features should evolve as they grow, avoiding sudden exposure to high-risk environments. Personalised services – which include social media, certain gaming and AI chatbots – must be prohibited for under 13s and all children protected and empowered up to 18.
- Default safety and privacy: Essential privacy and safety protections, especially for under-16s but for all children up to 18, must be on by default, with no option for them to be switched off.
- Holistic risk assessment: Age-appropriate design should take into account how a service works, who uses it, and how its features or business model amplify harm. Children's risk assessments should be dynamic, regularly reviewed and made public. They should also assess differential impacts on children with protected characteristics and vulnerabilities, including how platform design, recommender systems, reporting tools and moderation practices may compound these risks.
- Evidence-based design: Age-appropriate design should draw on robust research, harm data, and independent consultation with children, families and child development experts.

All proposed measures in the consultation should be subject to a full and transparent Child Rights Impact Assessment, to understand how they affect children's rights, everyday experiences, and potential inequalities - including for those with heightened vulnerabilities and protected characteristics. Children must be able to understand how policies affect them, ensuring that protections are not just theoretical but meaningful, accountable and grounded in real-world experiences.

2. **Remove the commercial incentives for harmful digital design**

Focusing only on age thresholds for individual features risks treating the symptoms while ignoring the cause: business models that rely on collecting and using children's data at scale to maximize engagement, attention and advertising revenue.

Design features such as infinite scroll, autoplay and push notifications should not be viewed in isolation. They are products of these attention-driven systems, designed to maximise time on platform and often undermining children's autonomy and wellbeing.

These business models determine how the platforms are designed and shape online environments in ways that drive harm to children. Raising the digital age of consent will not fix these deeper structural issues.

The Government must prohibit the use of targeted advertising, profiling and manipulative design features in services used by children, ensuring that companies cannot profit from practices that harm child users. As a first step, the Government should embed the Age-Appropriate Design Code (AADC) in primary legislation. Making its 15 standards mandatory would address how children's data is used and how services are designed, helping to restore children's agency while ensuring their safety, and realigning business models with children's rights and wellbeing. The Government should also amend the Online Safety Act to include a definition of safety by design and instruct Ofcom to bring in a code of practice to bring this into effect.

3. **Regulate AI systems rigorously**

AI presents risks to children that need to be addressed urgently and in a joined-up way. These risks go beyond harmful content and are already affecting children's development, behaviour, autonomy, and wellbeing. They cannot be managed through age limits or basic content filters alone. Instead, we need a clear, risk-based regulatory framework to protect children from AI systems that can shape behaviour, reduce agency, or amplify harm. This should include:

- Mandatory children's risk assessments

- Product testing
- Built-in safeguards reflecting children's vulnerabilities
- Transparency, accountability and enforcement mechanisms
- Protections embedded in design from the outset

4. **Strong leadership for online safety regulation**

Protecting children online requires clear leadership, coordinated action across regulators and accountability for outcomes. Parts of this responsibility currently sits across multiple bodies including the Government, Ofcom, the ICO, the CMA and others, but there remains a lack of joined-up strategy, particularly in relation to children's rights, wellbeing and online harms.

We propose strengthening independent leadership for children's online safety through the creation of a dedicated Online Safety Commissioner (or equivalent statutory leadership role). This role would not replace existing regulators, but would act as a champion for all children, ensuring their needs, rights and lived experiences online are consistently represented in regulatory and policy decisions. The role would have the authority to set the criteria for safety, wellbeing and age-appropriate design by convening experts on child development and safety and carrying out research. They would drive alignment between regulators, drawing on this work, and hold both industry and public bodies to account for outcomes.

The Commissioner would:

- Set the criteria for safety, wellbeing and age appropriate design by leading and commissioning independent research into children's experiences online, harms, and the effectiveness of regulatory and non-regulatory interventions.
- Work in partnership with schools, civil society, industry and government to develop and test evidence-based approaches to online safety and wellbeing.
- Support the co-development of digital literacy initiatives with children and young people themselves, ensuring that education and interventions are grounded in lived experience and not designed for children in isolation from them.
- Monitor and report on system-wide outcomes, assessing whether regulatory action is delivering measurable improvements in children's mental health, wellbeing, safety and overall online experience - so that success is judged by real-world impact, not procedural compliance alone. This should include identifying outcomes for vulnerable children and highlighting where further action is needed to ensure the same safeguards for all children.

- Identify gaps and overlaps in the current regulatory landscape and make recommendations to government on how to improve coherence and effectiveness.
- Support the Government to convene regulators and relevant government bodies (including Ofcom, the ICO and the CMA) to bring together a coherent, shared strategy on children's online safety and wellbeing, fostering alignment and regular strategic engagement across organisations.
- Set out a longer-term pathway for the Commissioner's office to one day serve an ombudsman-style function for children's online safety and wellbeing, focused on learning from lived experience and highlighting systemic issues over time.

Signed:

Organisations:

5Rights Foundation
Internet Watch Foundation
Plan International UK
Ditch the Label
The Children's Media Foundation
Internet Matters
Girlguiding
Children in Wales
Anti-Bullying Alliance
Childnet
Children's Law Centre
UK Safer Internet Centre
NSPCC
Catch 22
FlippGen
Family Action
End Violence Against Women
Breck Foundation
Online Safety Act Network
ECPAT UK
National Children's Bureau
Marie Collins Foundation
SWGFL
Royal College of Paediatrics and Child Health

Individuals:

Professor Sonia Livingstone, Director of the Digital Futures for Children Centre

Adele Walton, online safety campaigner