A JOINT STATEMENT OF PRINCIPLES
FOR FURTHERING THE PROTECTION OF CHILDREN ONLINE

These principles describe the baseline for a decisive, ambitious and proportionate legislative initiative to protect children from the preventable harms and exploitation to which they are routinely exposed via child-inappropriate features and experiences on social media and other digital services.

Safety as the price for access to children: Children should be protected from the harms posed to them by digital services with child-inappropriate characteristics by a targeted statutory measure. The effect of that measure should be that digital services, or separate parts of services, which cannot prove compliance with statutory minimum design safety and data transparency conditions should not be permitted to access children as users ('age-restricted' services).

Age-restricted services which fail to protect children in this way must face OSA-style deterrence penalties, while parents and children must face no penalties. The burden of protecting children from service-related harms must sit with those services, and should not depend on interventions from parents or from Ofcom, which is already bearing extensive responsibilities under the OSA.

Incentivising safety by design: The protections for children should be structured around a set of design safety and transparency conditions. Those conditions should be established and overseen by Parliament but made capable of developing *dynamically*, so that design safety can keep pace with and tackle new and evolving technologies and harms.

Those conditions should identify the design features and other characteristics of services that are harmful or otherwise not suitable for children in a way which can ensure that (i) design safety conditional access is targeted only at services or parts of services whose design features or other characteristics present a risk of harm to children, and (ii) service designers are given clear signposts and incentives, to encourage and facilitate the development of services which are suitable for use by children.

The statutory conditions for accessing children should address service characteristics which pose risks of harm to children including, at a minimum: (i) addictive or persuasive design features such as infinite scrolling, auto-playing, auto-queuing, public affirmation tokens, penalties for non-engagement, real time alerts and notifications, and (ii) any other risky features or functions identified in any Ofcom Register of Risks or in an internal risk assessment, stranger pairing and stranger contact facilities, recommending of OSA-defined illegal or child-inappropriate content, livestream broadcasts, location tracking, AI features raising risks of attachment or manipulation, non-compliance with data privacy laws, and poor enforcement of terms of service including minimum age limits. Relevant experts and authorities, including Ofcom, the Children's Commissioner,

and the Medical Royal Colleges should be able to input into processes for updating those conditions.

It must also be a condition for accessing children that digital services make relevant internal data available to independent researchers to facilitate monitoring and research.

Broad in scope, focussed in application: The conditional access requirement, and the design safety and transparency regime that underpins it, must be capable of applying not only to major social media services, but also to gaming services and other digital services where children tend to encounter harmful features, functions, content and people. It should be capable of applying to small services too, and must be defined flexibly enough to mean that other kinds of non-suitable digital services can be brought into scope.

Services using AI companion and chatbot features should be within scope of this child protection measure, so that children can be protected from encountering unsuitable forms of AI which can pose emotional or safeguarding risks; but legislation must also anticipate that other categories of child-inappropriate services will emerge.

OSA content moderation for children remains essential: As children will continue to be able to access the many services, large and small, which meet these statutory design safety and transparency conditions, the Online Safety Act content moderation duties must continue to apply to all OSA-regulated services as they do today. Digital services should not be excused from any existing child online safety duties. Amendments to boost the potency of the Online Safety Act regime, including a general duty of care for service operators overriding the OSA safe harbour, app store and device-level protections for children, and updates to Ofcom's investigatory and enforcement powers, should also be contemplated.

Limiting workarounds: A perfect water-tight regime cannot realistically be expected. Some children will seek out workarounds some of the time, and relevant services should anticipate this activity. Complementary legislative and policy measures should be contemplated both to encourage broader design safety principles across all online environments and to limit the most obvious and straightforward means for children to circumvent this protective legislative regime. Digital services must retain responsibility for the safety of children using their services regardless of how those children have accessed those services. Building societal consensus and using public messaging and digital education to nurture organic support and adherence to these measures should be the primary objective.

Timely public messaging: The public, professionals dealing with children, and parents and children in particular, must be equipped to understand how and why unsuitable services are to be restricted for children and teens, in ways that explain rather than dictate. A programme of public health messaging (including advice from the UK's Chief Medical Officers) should be used to build broader societal understandings of the harms and risks posed to children by engagement-driven business models and the persuasive

design characteristics of unsuitable services, as much as by the inappropriate content. In particular messaging should not refer to ‘banning’ children from services, or to blanket bans, and should instead focus on safe design as a baseline condition for services to be able to access children and young people as users.

Children and young people supported and heard: The digital and media literacy element of the curriculum should be updated promptly to aid development, at appropriate ages and developmental stages, of the skills that children will need to understand, anticipate and successfully navigate the risks they will encounter on adult services once they become ‘of age’. This should include age-appropriate units on service, algorithmic and AI literacy, and a granular understanding of engagement-driven business models and the ways in which personal data can be monetised by services.

The experiences and aspirations of children who will be affected by these restrictions, and of the young adults who will be exposed to unrestricted services, should be taken into account alongside the views of parents both when calibrating the design safety conditions and when periodically reviewing the effectiveness of the regime as a whole. So should the views of children’s charities and other relevant safeguarding and medical experts be heard.

An independent authority: An independent authority or commissioner, with an overriding primary duty to promote children’s wellbeing, could be formed to play a coordinating, monitoring and directional role, working alongside and complementary to the existing roles of Ofcom and the Children’s Commissioner. Its objectives and powers should be statutory. It would need to be operationally independent of government, as far as possible inoculated against industry influence, and funded by annual industry levies.

This independent authority could be given powers to require the provision of information directly from services which are being accessed by children. In addition to analysing the response of digital service providers to this targeted statutory measure, the authority could have powers and objectives to collect information about the experiences of parents, teachers, children and young people, and others affected by requirements for age-based restrictions, and to highlight emerging risks and other critical developments as the online landscape evolves. It could also be given investigative and enforcement powers, including a power to intervene on short notice with injunctive powers if it identifies services posing a risk of serious harm to children.

* * *

April 2026

Signatories

This Joint Statement describes the baseline for a decisive, ambitious and proportionate legislative initiative to protect children from the preventable harms and exploitation to which they are routinely exposed via child-inappropriate features and experiences on social media and similar platforms.

By adding their names to this frontpage, signatories are indicating support only for the principles set out in the Joint Statement which appears below, rather than for any specific legislative amendment or other legislative process.

The following organisations and individuals support the Joint Statement:

Organisations
Anti-Bullying Alliance
Avaaz Foundation
Be Challenge Aware
Brianna Ghey Legacy Project
BulliesOut
CEASE (the Centre to End All Sexual Exploitation)
Centre for Protecting Women Online
Centre of Excellence in Child Trauma
Children and Young People's Mental Health Coalition
Close Screens Open Minds
Coram
Centre for Young Lives
FLIPPGEN
Generation Focus
Health Professionals for Safer Screens
Internet Matters
Internet Watch Foundation
Jools' Law
Mental Health Foundation
Mumsnet
Parentkind
NASUWT - The Teachers' Union
National Children's Bureau
National Council of Women GB
NEU
NSPCC
One Collective Power
PAPAYA
Ripple Suicide Prevention Charity
SafeScreens
Shout Out UK
SWGfL
Unplug.Scot
Unplugged Coalition

YoungMinds
5Rights Foundation

<u>Individuals</u>
Lord Nash
Baroness Benjamin
Baroness Cass
Baroness Berger
Alice Hendy MBE
Amanda Stephens (Mother of Olly Stephens)
Anna Ford (Mother of Madelyn)
Areti Nicolaou (Mother of Christoforos)
Beth Layton (Mother to Elsa Layton-Jones)
Chris Ford (Father of Madelyn)
Eliza Gabb (Mother of Sky Gabb)
Ellen Roome MBE (Mother of Jools Sweeney)
Esther Ghey (Mother of Brianna Ghey)
George Nicolaou (Father of Christoforos)
Hollie Dance (Mother of Archie Battersbee)
Ian Banyard (Father to Lacey Banyard)
Lisa Kenevan (Mother of Isaac Kenevan)
Lorin LaFave (Mother of Breck Bednar)
Louise Gibson (Mother of Noah)
Mariano Janin (Father of Mia Janin)
Matthew Sweeney (Father of Jools Sweeney)
Michael Absalom (Father of Kady Absalom)
Michelle Barrett (Mother of Kibi Wade)
Michelle Gardner (Stepmother of Kibi Wade)
Penny Banyard (Mother to Lacey Banyard)
Ruth Moss (Mother to Sophie Moss)
Stuart Stephens (Father of Olly Stephens)
Tanya Absalom (Mother of Kady Absalom)
Terry Layton (Father to Elsa Layton-Jones)
Professor Sonia Livingstone OBE
Maeve Walsh (Director, Online Safety Act Network)