NSPCC

Ofcom's Protecting Children from Harms Online Consultation: NSPCC Response – Executive Summary

The Online Safety Act is a vital child protection measure. Ofcom's continued implementation of the regulation is critical for bringing its powers into force, and ensuring services can no longer evade adhering to the new duties and making child safety a priority.

We welcome the increased focus by Ofcom on early harm prevention in these Codes of Practice. In particular, strong measures on recommender systems, implemented effectively, will help ensure that children are no longer fed dangerous and inappropriate content.

As with the Illegal Harms Consultation, however, this must be seen as a first step in building a stronger regulatory regime. There are notable gaps in Ofcom's proposals. Above all, there must be an increased focus on ensuring that Codes of Practice promote best practice and incentivise services to take an innovative approach to safety solutions.

Our full response sets out our detailed assessment of Ofcom's proposals. In this document, we summarise key areas which must be a priority for future action to strengthen the regulation for children – alongside our recommendations for the Illegal Harms Consultation. These areas are:

1. **Enforcing minimum age limits**. All services who set a minimum age limit must ensure that users who are below this age are not able to use their platform. Children who are below minimum age limits are currently at significant risk online. Ofcom must require that platforms address this.
2. **Addressing all identified risks**. It is highly concerning that Ofcom have identified significant risks to children in the Register of Risks, but these are unaddressed in the Codes of Practice. The Act prescribes that Codes are 'safe harbours' for services. Without a change to the Act by Government, or the naming of more comprehensive, outcomes-based measures by Ofcom, features and functionalities which are proven to put children at risk will continue to go unaddressed.
3. **Utilising innovative technologies and approaches**. There must be a greater use of proactive technologies, which can introduce friction into harm pathways and ensure harmful content and behaviour is swiftly identified. Otherwise, children will continue to carry the burden of having to protect themselves online.
4. **Tackling harm in private messaging**. As public spaces improve their safety measures, there is a significant risk that illegal and legal harms will migrate to private messaging services, which already pose a major risk to children. Ofcom must pre-empt this and introduce robust measures for private messaging services now.
5. **Aligning measures for the Illegal and Legal Codes**. It is vital that the strongest measures are in place to tackle the most egregious risks to children online, including child sexual abuse and exploitation (CSEA). All measures which could strengthen protection from CSEA which are included in this Code must be added to the Illegal Harms Codes too.

Action across all these areas must be underpinned by engagement with children and young people. As we highlight throughout our response, insight from children is critical to identifying emerging risks and defining what works to keep them safe. Whether it is understanding what age-appropriate experiences look like, the impact of new technologies,

or assessing the connection between different risks, the views and experiences of children and young people are critical to developing informed analysis and solutions which are based in the reality of children's online lives.

Ofcom have rightly recognised the important insight which children and young people have to offer. **As a next step, this must be embedded in the regulatory regime through the introduction of formal mechanisms to ensure children are consistently able to inform and shape decision-making.**

Whilst we welcome the steps Ofcom have taken to include children's voices, there are limitations to their approach. In particular, we understand the focus of the deliberative engagement is on Ofcom's suggestions and not child-led in understanding what solutions will work best for them. As Ofcom is directing this work, it is also not an independent check on the regulator, and risks being used to rubber-stamp current plans rather than to challenge and shape different proposals.

The NSPCC recently worked with Baringa to understand the features of successful and meaningful user engagement in regulatory regimes, which should inform the design of formal engagement mechanisms for children.[1]

Enforcing minimum age limits

Children who use services below the minimum age limit face significant risk of both illegal and legal harms on these platforms. Research shows that children who are many years below the minimum age for social media platforms are able to create accounts and use these services, and as a result face significant harm including seeing inappropriate content, online bullying and harassment, and child sexual abuse.

> "There's this group of girls in my school who bully me for how I look. They're determined to make my life hell online too: they keep adding me to these Snapchat groups where they say nasty things about me. When I block them, they create new fake accounts, and I can't stop being added to new groups. I feel like nobody likes me and that I'll always be the unpopular kid." Call to Childline from a girl, age 11[2]

The risk posed by underage access to services for young children is great, and demands that Ofcom take explicit action in the Codes of Practice to address this. Through a combination of age assurance and age estimation technologies, it is possible for services to understand, to a much greater degree accuracy than is currently the case, the age of children using their services. This could include age estimation based on real-time photos, the use of AI technologies, or interoperable solutions such as digital wallets.

Given implementing age assurance to distinguish between children of different ages is not currently widespread, Ofcom would need to ensure approaches by services are safe, accessible and privacy-preserving.

---

[1] NSPCC and Baringa (2024) Putting children's voices at the heart of online safety regulation: a study of user representation mechanisms in regulated sectors. London: NSPCC.

[2] Please note that Childline snapshots used in this document are based on real Childline service users but are not necessarily direct quotes. All names and potentially identifying details have been changed to protect the identity of the child or young person involved.

NSPCC

Key recommendation: We strongly urge Ofcom reconsiders their approach to minimum age limits in the Codes. Next steps must include setting out the range of options available to services, adding a specific requirement in the Codes, and incentivising innovation to increase the range of solutions available.

Equally, Ofcom could swiftly use their enforcement powers to tackle platforms which do not uphold their minimum age limit, highlighting that this is a priority area for action and proving that this framework will be impactful for children.

Addressing all identified risks

We continue to be concerned with the approach Ofcom is taking to recommending new measures in the Codes of Practice. The high-evidential threshold for recommending measures is a consistent barrier in enabling Ofcom to push innovative, best practice solutions that would see a step change in the approach of services to safety by design.

It is highly concerning that the result of this approach means that Ofcom has identified significant risks to children in the Register of Risks, but these are unaddressed in the Codes of Practice. Where the evidence is clear that features and functionalities are causing harm to children, services must be required to address these. This does not mean that Ofcom must always propose specific solutions. Instead, we have argued that Ofcom should include more outcomes-based measures to the Codes, requiring services tackle the risks posed by certain functionalities or features (such as choice architecture) without setting out the exact steps that must be taken.

It is particularly important that Ofcom reconsiders this approach because of the long-term precedent it risks setting. Not only does the current approach mean Ofcom have not addressed all identified drivers of harm in the Codes, but it also risks removing the incentive for platforms to invest in and rollout ground-breaking safety measures. As platforms will be deemed compliant by only implementing the Code measures (due to the Act making Codes a 'safe harbour'), it will be difficult for Trust and Safety teams to justify investing in new solutions. Internal decision makers may favour rolling out older technology recommended in the Codes over new, innovative measures, regardless of how impactful.

Key recommendation: Ofcom should reconsider their evidence threshold and include more outcomes-based measures in the Codes of Practice to ensure they are able to drive action on all identified risks to children online.

Utilising innovative technologies and approaches

A fundamental purpose of the Online Safety Act is to move the burden away from children from having to protect themselves, by embedding safety into the design of platforms. Achieving this requires services to invest in and implement proactive, preventative tools which ensure harm is detected and disrupted before it impacts children.

Ofcom's measures on recommender systems are an important and welcome example of tackling harm upstream and ensuring the design of services is safer for children. In future Codes, there must be a much greater use of proactive tools which can prevent, detect, and disrupt harm. These tools will significantly enhance the content moderation measures, and strengthen Ofcom's approach to harms such as bullying and harassment.

Many of the Code measures build on and adapt existing approaches to safety by services. This risks an overreliance on developing ineffective systems, rather than setting out what genuine best practice would look like.

For example, looking at reporting, Ofcom reject offering children the option to opt out of receiving communications relating to a complaint, in case this causes further distress, on the grounds that they have not seen evidence that this is a problem and evidence shows children want more information about reporting, rather than less. However this is the wrong conclusion to draw from the evidence. Children are currently unlikely to raise that they are distressed by information shared in report updates not because this is not a risk, but because they rarely receive any follow-up at all. Similarly with trusted flaggers, there is currently limited evidence of their efficacy because services do not utilise them effectively – this does not mean they don't have significant potential.

Key recommendation: Ofcom should base Code of Practice Recommendations on what best practice should look like, including a greater use of harm prevention tools. Children and young people should directly inform a clear vision of what platforms which are safe by design for children would look like.

Tackling harm in private messaging

Children experience significant harm in private messaging. Calls to Childline show that children are exposed to Primary Priority and Priority Content in private groups – including bullying and abuse, and exposure to self-harm and suicide content and sexual content.

> "I got added to a WhatsApp group where people post selfies of other people. Everyone else in it rates how ugly they are and tells them to kill themselves. I'm worried that I'll be identified just from being in the group" Call to Childline from a young person, aged 14

As Ofcom have not recommended the use of any proactive technologies in the Codes, all measures apply to private messaging. In reality, however, private messaging services will have very limited duties under these Codes, despite the harm which occurs on them.

There is a significant risk that, as public spaces improve their safety measures, illegal and legal harms will migrate to private messaging services. The risk that private messaging already poses to children's safety will be exacerbated, and harms will escalate as there are not sufficient measures in place to meaningfully tackle harmful content and behaviour in these spaces. Whilst we recognise there are limitations to the Online Safety Act, there is significantly more Ofcom could do to hold these sites accountable for improving their services.

Key recommendation: Ofcom must pre-empt the risk of harm increasingly migrating from public to private spaces and introduce robust measures for private messaging services now.

Aligning measures for the Illegal and Legal Codes

It is vital that the strongest measures are in place to tackle the most egregious risks to children online, including child sexual abuse and exploitation. We welcome that for many of the relevant new measures added to this Code, Ofcom is recommending they are added to the Illegal Codes too.

There are, however, notable gaps to this which must be addressed.

Firstly, Ofcom must require that services with a risk of grooming use highly effective age assurance (HEAA). Ofcom recognised in the Illegal Harms Code that the grooming measures would be considerably more effective following the introduction of HEAA. Given the severity of the risk posed by grooming, it is vital that the measures to tackle it are as robust as possible. As the success of the grooming measures is reliant on identifying child users, it is both essential and highly proportionate to require that services with a medium-high risk of grooming are using HEAA.

Secondly, the recommendation that services provide children with the option to accept/decline a group chat invitation should also be applied to the Illegal Harms Codes too, for services that pose a risk of child sexual abuse material (CSAM) or grooming. There is significant evidence to show that group chats often contain a mixture of illegal sexual content (including CSAM) and harmful content. For example, a BBC investigation found that children in the North East were being added to malicious WhatsApp groups promoting self-harm, sexual violence and racism.[3] Calls to Childline also reinforce that group chats can be used for, and be dedicated to, illegal material. This is an important measure which will benefit from being applied as widely as is appropriate.

As well as extending the scope of some measures, greater consideration should be given to the links between illegal and harmful content. As noted above, children often experience legal and illegal harms simultaneously.

> "I've been thinking about stuff that happened to me a few years ago. There was so much going on in my life, I'd just started self-harming and the only place I could escape was on Discord. Some of the people on there were total creeps but it didn't matter who they were, I just needed someone to talk to. There was this guy who was 30 or something. He added me and after chatting for a while, he would ask me to, like, self-harm for him and send pics of it, that type of thing. Mum eventually found out and said I was groomed." Call to Childline from a girl, aged 14

For example, some platforms will be a high risk for both sexual content and for image-based sexual abuse, with children exposed to a mix of pornographic material, non-consensual intimate imagery and CSAM.[4] Another example is reports that on some forums, adults are grooming children online to sexually extort them and to coerce them into dangerous acts including self-harm.[5] Calls to Childline also highlight the interplay between harms. In some cases all activity may be classed as illegal, but risk assessments will ultimately be stronger if services consider the relationship between different harms and introduce holistic mitigations.

Key recommendation: All relevant measures from the Children's Safety Codes should also be added to the Illegal Harms Code. Through the risk assessment process, services should be required to assess the links between illegal and harmful content and to ensure they have clear systems in place which ensure this material is swiftly identified, properly reported, and that children have holistic protections and support.

---

[3] Downs, J. and Lindsay, M. (2023) Nine-year-olds added to malicious WhatsApp groups. BBC News.
[4] Revealing Reality (2023) Anti-social Media: The violent, sexual and illegal content children are viewing on one of their most popular apps.
[5] Federal Bureau of Investigation (2023) Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material.

NSPCC

The NSPCC is the UK's leading child protection charity with over 130 years in experience safeguarding children from harms. A driving force in the passage of the Online Safety Act, we are committed to ensuring every child is safe online.

We have significant knowledge and expertise, based on a strong research and evidence base and direct work with children, and are committed to using this to advocate for the development of a strong, ambitious, regulatory framework which centres children's experiences and tackles the full range of harms children experience online.

To discuss the NSPCC's response to Ofcom's Protecting Children from Harms Online Consultation further, please contact Rani Govender (Policy and Regulatory Manager) – rani.govender@nspcc.org.uk.