parentzone

Consultation response

Proposed amendment to Ofcom's Illegal Content Codes of Practice: additional user controls

parentzone

About Parent Zone

Parent Zone is an organisation that sits at the heart of digital family life, providing advice, knowledge and support to shape the best possible future for children as they navigate a digitised world. Founded in 2005, we have collaborated with many organisations who share our vision, remaining responsive to the continually developing nature of digital technologies, and how they intersect with family life. We recognise enormous opportunities, whilst understanding the challenges that accompany them.

You can read Ofcom's consultation and proposed changes to their Illegal Content Codes of Practice, here.

parentzone

Question 1: Do you agree with our proposal? Provide any evidence to support your answer.

We welcome Ofcom's responsiveness to previous feedback from organisations, many of which have highlighted the need to expand existing measures. We do however have a number of concerns with the proposal.

Our concerns relate to the many limitations of user controls, including ICU J1 (blocking and muting) and ICU J2 (disabling comments) and the measures' ability to keep pace with emerging tech including wearables and XR. We are also worried that the exemption of certain smaller services – which are often some of the highest risk to users – amounts to a significantly harmful loophole. Finally, we are concerned about the ambiguity of the language used by Ofcom in this proposal and what this might ultimately mean for user safety.

Limitations of user controls

Our research, and that of other researchers, has shown that user controls do not always improve user safety. Our report into parental controls and user empowerment tools revealed that they can be confusing to grasp and time-consuming to implement effectively. In assessing just 8 platforms we found a total of 121 tools.[1]

Tools with similar functions often change in how they are labelled across platforms which can make them more confusing and complex to select. At the same time, tools with the same names or similar icons can work differently depending on the platform. Tools within the same platform can also change over time – close to 30% of the tools we evaluated had changed in the last year.[2]

These limitations, particularly around blocking, reporting, and disabling comments are critical and should be explained to services to prevent the risk of complacency or a sense of the job being 'over and done' once tools are implemented.

Furthermore, it is reasonable to assume that if an adult finds it difficult to understand and utilise user controls then a child will too, possibly to a much greater extent. Ofcom's own research supports this assumption, finding that children's awareness of tools is not just lower overall, but that they also need more motivation to begin engaging with these tools in the first instance.[3]

---

[1] Online safety tools — a false hope?

[2] Ibid.

[3] Using Behavioural Insights to Engage Children with User Support Materials | Ofcom

It is also possible that children are overconfident in their ability to deal with difficulties they experience online *without* using controls and tools. They may also be worried that an individual they mute or block (ICU J1) will know that the child has done so and that there will be consequences like further harassment. A child user may also be worried that disabling comments (ICU J2) will overly diminish the enjoyment they get from a service.

These factors could all hinder the activation of user controls – leaving the children they are intended to protect no safer and, worse, leaving parents assuming the platforms are safer when the user experience simply is not.

We would also flag that it is unlikely user controls that were largely designed for use by adult users will be effective at protecting younger users without additional support mechanisms. In cases where a child has been exposed to harassment or harmful content, additional information and the signposting of support and/or reporting options (as well as follow-ups from the service itself) would all be important. Adding this additional requirement would be a welcome addition in Ofcom's guidance or 'best practice' for services. Parent Zone created a 'digital pattern library' to help platforms support digital resilience through design. We would strongly recommend a similar pattern library approach to support these proposals.

One clear way to improve how much – and how effectively – these tools are used is for them to be consistent across platforms. This means that they function similarly and are also worded using consistent language and visuals. Whilst it's encouraging to see Ofcom note that "information must be easy to find and comprehensible based on the likely reading age of the youngest individual permitted to use the service", over 7 million adults in the UK struggle to read at a level above an 'average nine year-old'.[4] For language and information to actually be 'comprehensible' services should use this as a ceiling. We are also hesitant to believe that some smaller services will comply with this call for ease and comprehensibility when we repeatedly see dense language deployed by services alongside dark pattern design and deliberate obfuscation of problematic features.

In short, whilst we welcome any moves to ensure that basic user controls are in place across more platforms, it is important to recognise that they aren't a fix-all and should not be considered such either by Ofcom or services in scope of Ofcom's codes. When appropriately designed and implemented by services these tools *may* help improve user safety, but they can be detrimental to safety (rather than imperfectly helpful) when not.

---

[4] Health literacy: how can we improve health information?

Changing digital landscape

Ofcom has stated that its implementation of the Online Safety Act (OSA) is iterative, and we are pleased to see that additional measures ICU J1 and ICU J2 are an example of this process.

Despite this iterative and responsive approach, specific and detailed consideration needs to be given to how the above controls will be effective in new technologies and digital environments like virtual reality (VR) and extended reality (XR).

Specific harms like harassment can be more problematic or uniquely challenging in VR and XR settings and in the context of new digital landscapes that include AI-enabling wearables. We are already seeing new harms including 'virtual rape' or 'meta-rape', with research showing how these more physically invasive forms of virtual abuse can be experienced by users.[5]

This proposal needs to consider how muting, blocking or comment-disabling functions can be used in environments that are increasingly immersive, and where a difficulty to 'disengage' when being harassed and harmed will render these tools ineffective. The frictionless nature of these experiences can also make certain tools harder to surface as part of the overall user experience.

This is not to say that additional measures cannot be effectively implemented in these contexts. Research into 'social virtual reality' shows that "Reactive tools like muting and blocking" are widely used by adult respondents (61%) but that this is largely driven by users' familiarity (i.e. their experience with these features on other platforms).[6]

However, relying on familiarity from other digital experiences to drive usage of tools in emerging and novel tech contexts is not an adequate long-term approach. Nor is it an approach well-suited to child users who may be yet to develop levels of familiarity.

Future-proofing Ofcom's codes is essential. Ofcom must be forward-facing rather than simply responsive when it comes to these additional user control measures.

---

[5] From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse | Oxford Journal of Legal Studies

[6] Beyond Mute and Block: Adoption and Effectiveness of Safety Tools in Social VR, from Ubiquitous Harassment to Social Sculpting

parentzone

Categorisation of services

We naturally support further well-designed safety measures applying to a greater number of services. Ofcom's definition of a 'large service' being those with +7m users (or 10% of the UK population), has left many thousands of smaller, high risk platforms out of scope of certain measures. It is equally clear that many services falling outside this bracket aren't 'small' at all, and should therefore offer users additional protections against harmful content and interactions, like those set out in Ofcom's proposal.

We do question Ofcom's suggestion that "smaller services with fewer than 700,000 monthly UK users and a medium risk of harm would struggle to implement the measure in a way that increases protection from illegal content without material adverse effects for users".

Firstly, we would ask what a service with a 'medium risk' of encouraging or assisting suicide (or indeed other priority offences and content) actually looks like. We would argue that a pro-suicide forum with only a dozen members should absolutely fall under the scope of regulation. This seems commonsensical given the standards that are applied offline. For example, every children's toy – whether mass-produced and intended for a mass audience or boutique and limited in number – needs to meet reasonable safety standards. Under this proposal it seems that some services are entitled to say 'as we're small, it's okay that we pose a threat to children'.

Categorising services in this way also produces additional, unwanted consequences. Parents will be unable to determine if a service has these user tools and is therefore, in theory, 'safer' without somehow accurately checking the user base of the service, or using it themselves.

This is doubly problematic as smaller (<700,000 users) medium-risk services are less likely to be on a parent's radar to begin with. These lesser-known and risky services are ones which, ironically, safety measures like ICU J1 and ICU J2 should definitely apply to because of these expected gaps in parents' awareness.

These concerns are all compounded by the fact that the enforcement of the OSA is likely to mean children migrate to these smaller, less-regulated and known services, rather than larger services with highly effective age assurance (HEAA) and other safety measures in place.

We similarly challenge Ofcom's premise that these smaller (<700,000) services will be less able to implement additional measures. Difficulty of implementing controls should not be prioritised over children's safety. Similarly, with organisations – such as ROOST –

explicitly helping services implement these exact sorts of child safety tools, there seems little practical excuse for services big or small to shirk a responsibility for user safety and to implement additional measures.

Ambiguous language

Our final concern relates to the language used by Ofcom across its codes and guidance, and how that language may interact with this proposal specifically.

After publishing the children's risk assessment guidance and Protection of Children Codes of Practice in April 2025, Ofcom stated that all user-to-user and search services must assess whether they are likely to be accessed by children, and that platforms likely to be used by children will need to assess risks posed and take action to protect them – which "may include" using HEAA.

Whilst this seems straightforward, it leaves open the possibility that the measures a service takes in response to their children's access and children's risk assessments won't include implementing age assurance.

This interpretation of Ofcom's codes is worrying when applied to this current proposal on user controls. We are concerned that it may remain possible for a service (of a certain size and risk level) to implement user controls ICU J1 and ICU J2 rather than implement HEAA. This may result in children being allowed access to risky and harmful services with the onus on child users keeping themselves safe through controls such as ICU J1 and ICU J2. Under this particular interpretation, this scenario would seemingly be compliant with Ofcom's codes.

If this interpretation is *incorrect* – which, we stress, is entirely possible – then it nevertheless raises a question around the language used by Ofcom and its clarity. After consulting with colleagues in the sector, they too are unsure as to what the exact consequences of Ofcom's proposal will mean, and whether the scenario described above would be possible or not. Without clear, unambiguous language services themselves may incorrectly interpret Ofcom's codes – even with intentions of compliance in mind.

Less optimistically, the opaqueness of the codes may be used by certain services to their own benefit, i.e. to continue 'as normal' for a longer period of time. Without explicit clarification from Ofcom, this proposal could result in further instances of this and therefore continued harm.