Consultation response form

Please complete this form in full and return to protectingchildren@ofcom.org.uk.

Consultation title	Consultation: Protecting children from harms online
Organisation name	5Rights Foundation

5RIGHTS FOUNDATION

Ofcom: Protecting children from harms online

5Rights Foundation consultation response

17 July 2024

Summary

5Rights acknowledges the scale of Ofcom's task in producing the Children's Safety Code of Practice – one of the first of its kind in the world. However, we remain concerned – as we set out in our response to the draft Illegal Harms Code of Practice[1] – that Ofcom's approach does not yet fulfil the promise of a "reset for children's safety",[2] nor does it reflect the scope and purpose of the Online Safety Act,[3] statements made by the Government in Parliament,[4] or promises made to children and parents.[5]

These draft proposals fall short because:

- The Code does not reflect the overarching principle (set out in Section 1 of the Online Safety Act)[6] that services must be made "safe by design" and fails to address risks created by high-risk features and functionalities such as direct messaging and livestreaming.
- The measures services are required to take in order to claim 'Safe Harbour' in Volume 5 (the draft Children's Safety Code) do not address all the risks identified in Volume 3 (the draft Children's Register of Risks).
- The Code fails to require services to be age-appropriate by design[7] – meaning there is no difference between services offered to a 7-year-old and a 17-year-old.
- The Code does not require services to take any steps to enforce – or even set – minimum age requirements.[8] This means that millions of children will continue to access services that the service provider themselves deem inappropriate.

The structure and approach of the Illegal Harms Code of Practice has been adopted in this Code in order to ensure alignment – including many of the risk mitigation measures. In light of this, unless the Illegal Harms Code is radically amended before the final Code

---

[1] 5Rights Foundation (2024) *Ofcom must rethink Online Safety Act Illegal Harms Code of Practice*

[2] Ofcom (2024) *Tech firms must tame toxic algorithms to protect children online*

[3] s.1, Online Safety Act 2023

[4] Lord Parkinson of Whitley Bay, 19th July 2023, Online Safety Bill, Report Stage (5th Day), Columns 2418-2419

[5] Department for Science, Innovation and Technology (2023) *UK children and adults to be safer online as world-leading bill becomes law*

[6] s.1, Online Safety Act 2023

[7] Vol. 5, 15.319 & Vol. 5, 15.317

[8] Vol. 5, 15.314 & Vol. 5, 15.19

is submitted to Parliament, this the Children's Code will inherit the same that problems we, and others in the sector, raised in our response to those proposals.[9]

Ofcom must look across both Codes to ensure the following key issues are addressed in order to meet the expectations of parliamentarians, child safety advocates, children and the public. Ofcom must:

1. **Require regulated services to take a safety by design approach (as required under s.1(3)(a) of the Online Safety Act)[10] by:**
   - Embedding the overarching duty in s.1 of the Act that regulated companies must be safe by design and provide a higher standard of protection for children than adults throughout the Codes and measures.
   - Addressing risk created by *all* aspects of service design, including features and functionalities (as required under s.12(8)(b) and Schedule 4 of the Act).
   - Mandating "by design and default" measures for *all* risk categories including features and functionalities.

2. **Revise the measures in the Code so that 'Safe Harbour' is only given to services that mitigate and manage all risks identified in Volume 3 (draft Children's Register of Risk) by:**
   - Reshaping measures so that they are effective and futureproof rather than process-based 'micro measures' that are focused on today's services.
   - Make 'Safe Harbour' protections conditional on regulated services making good faith, best practice efforts to manage *all* risks identified in their risk assessment – even (and especially) when there is no corresponding measure in the Code.
   - Requiring services to switch off access to risky or age-inappropriate features, functionalities or content by design where a risk has been identified for one or more age group and sufficient mitigations cannot be found until suitable mitigations can be identified.

3. **Require regulated services to give separate consideration to children in different age groups by implementing age-appropriate design (as required under s.11 and s.12) by:**
   - Setting measures about age-appropriate access to content, features and functionalities (as opposed to only protecting children from 18+ content), noting the decades of evidence that children of different age groups have different capacities to tackle, understand or even identify risk and/or behavioural norms.

4. **Require regulated services to set and enforce minimum age requirements by:**
   - Requiring services to specify a minimum age requirement for access to a service and to high-risk features and functionalities in their terms and conditions.

---

[9] Online Safety Act Network (2024) *OSA Network statement on illegal harms consultation*

[10] s.1, Online Safety Act 2023

- Requiring services to enforce their minimum age requirements *effectively*. This can be through effective privacy-preserving age assurance methods and processes and is not limited to age verification.
- Expanding guidance on age assurance to cover age checking on age-appropriate services as well as 18+ services.

5. **Require Ofcom to fully identify the limits of its regulatory powers that prevent it creating comprehensive codes of practice. To the extent that its powers are insufficient to fulfil any aspect of the Act, Ofcom must report this to the Secretary of State for Science, Innovation and Technology:**
   - Ofcom must review and publish its current interpretation of its powers under the Act.
   - To the extent that the powers are insufficient, Ofcom must report this to the Secretary of State so that the regulation can achieve the aims of the legislation and meet the reasonable expectation that the Children's Safety Code will protect children.

Full analysis of the five recommendations is set out in the section on Volume 5 below.

Consultation response

Volume 2 – Children's Access Assessments

We agree with the approach Ofcom has taken in casting the net widely when determining which services are in scope of the child safety duties. We also welcome Ofcom's consideration that the Children's Access Assessment should dovetail with that of the Age-Appropriate Design Code.[11]

Volume 3 – Draft Children's Register of Risks and draft Guidance on Content Harmful to Children

We welcome:

- Ofcom's proposal to include body image content and depressive content within the category of Non-Designated Content (NDC), and Ofcom's recognition of the harm the cumulative impact of this content can have.
- Ofcom's research in this volume sets out how the design of service, in particular its functionalities,[12] affects the level of risk of harm that might be suffered by children.[13] We regret that this is not addressed in Volume 5 (see below).

[11] Information Commissioner's Office (2021) *Introduction to the Children's code*
[12] See: s.233, Online Safety Act 2023 for a full list of features and functionalities
[13] As required under s.11(6)(e), Online Safety Act 2023

- Ofcom's position is that risk of harm to children varies depending on the age and development stage of the child.[14] Again, we regret that this is not reflected in Volume 5.
- The research Ofcom has carried out in support of this volume, particularly regarding the variations in risk profiles for children at different ages and stages and on children's online 'user ages', provides a good understanding of how children use the internet in reality.
- We strongly support the recommendation of the Domestic Abuse Commissioner[15] for the inclusion of misogyny as its own section in the Children's Register of Risk, in light of the multifaceted way this can manifest in online spaces.

We are concerned that:

- Ofcom has concluded that *all* Primary Priority (PPC) and Priority Content (PC) is harmful to *all* children irrespective of age. This does not reflect the evolving capacities of children and the need to take a more nuanced approach to older children's right to explore complex themes.
- Ofcom's analysis of 'Governance, Systems and Processes' does not include features and functionalities as an aspect of service design (as opposed to just being an amplifier of content risk). This fails to reflect the Act[16] and appears to have had the knock-on effect that none of the measures in Volume 5 relate to access to, or default settings for, features and functionalities.[17]
- Ofcom has not adequately articulated the risk posed by features and functionalities that affect the amount of time children spend on services and has concluded that "more research is required in this area."[18] We urge Ofcom to take into consideration the considerable research by Dr Amy Orben[19] from the MRC Cognition and Brain Sciences Unit, University of Cambridge, that clearly shows how persuasive design features individually and collectively impact on children's time and undermines aspects of their wellbeing.
- We would also point Ofcom to the evidence 5Rights has submitted to each phase of evidence gathering to inform the Codes of Practice which provides detailed information of how features and functionality heighten risk to children, including:

[14] See: Vol. 3, 6.6-6.8 & Vol. 3, 7.15

[15] See: Domestic Abuse Commissioner (2023) *Domestic Abuse Commissioner's Response to Ofcom's Call for evidence: categorisation – research and advice*

[16] See: s.12(8)(b), Online Safety Act 2023

[17] The five default settings requirements in Vol. 4 of the draft Illegal Harms Code of Practice (which relate to the visibility of child users) would apply (see: Chapter 18) but these are defaults only, they do not apply at a feature – as opposed to settings – level, they do not address access to features and do not consider age-appropriate design principles

[18] Vol. 3, 7.13.20

[19] Turner, G., Ferguson, A. M., Katiyar, T., Palminteri, S. & Orben, A. (2024) *Old strategies, new environments: Reinforcement Learning on social media*, DOI: 10.31234/osf.io/f5cjv. In particular, we refer to Table 1, *Taxonomy of social media affordances most relevant to the Reinforcement Learning process*, pp. 4-5.

- Call for evidence on Illegal Harms, September 2022;[20]
- Call for evidence on Children's Safety Duties, March 2023;[21] and
- Call for evidence on Categorisation, September 2023.[22]

Volume 4 – Governance and accountability and Children's Risk Assessment Guidance and Children's Risk Profiles

We welcome:

- The four-step (identify, assess, manage and report risk) approach to the Children's Risk Assessment.[23] This approach reflects best practice.

We are concerned that:

- The 'Safe Harbour' mitigations create a far less effective route to compliance as it does not cover functionalities, enforcing minimum age limits, age-appropriate design, or many of the risks that have been identified in Volume 3. This will result in a Code that does not meet children's safety or needs and will act as a drag on safety innovation (see analysis of Volume 5 below).

Volume 5 – Draft Children's Safety Code of Practice

1. Require regulated services to take a safety by design approach as required under s.1(3)(a) of the Online Safety Act:

Section 1[24] sets out the purpose of the Act and the overarching duties on regulated services. These include the following key provisions relevant to children:

> [This Act] "*imposes duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate and manage the risks of harm (including risks which particularly affect individuals with a certain characteristic) from—*
>
> *(I) illegal content and activity, and*
>
> *(ii) content and activity that is harmful to children*" (s.1(2)(a))
>
> "*Duties imposed on providers by this Act seek to secure (among other things) that services regulated by this Act are—*
>
> *(a) safe by design, and*
>
> *(b) designed and operated in such a way that—*
>
> *(i) a higher standard of protection is provided for children than for adults…*" (s.1(3)(a)-(b)(i))

[20] 5Rights Foundation (2022) *Call for evidence: First phase of online safety regulation*
[21] 5Rights Foundation (2023) *Call for evidence: Second phase of online safety regulation*
[22] 5Rights Foundation (2023) *Categorisation: Research and advice*
[23] Vol. 4, 12.32-12.50
[24] s.1, Online Safety Act 2023

These purposes and duties have effect over the whole of the Act, which means that further sections and duties must be read, and Codes drafted, in reference to them. This is not reflected in the current draft of the Code, illustrated by the fact the Code concerns itself almost exclusively with content and contains very limited provisions that relate to features and functionalities – despite repeated assurances from the despatch box that 'content' meant 'content and activity' and that the Act would cover all online functionality.[25]

For example, Ofcom has not included any measures relating to restricting access to high-risk features or functionalities for all children or children in certain age groups. This is even in cases where Ofcom's own analysis in Volume 3 has found that these are high risk. Whilst 5Rights recognises that Ofcom has included general measures (for example on governance or user controls), they are not sufficient to address the risk of, nor targeted specifically at, high-risk features and functionalities. For example:

Livestreaming:

- Risk posed by this functionality: Ofcom sets out in Volume 3 how this functionality presents a risk of serious harms to children, including where children have seen a video of someone taking their own life,[26] where they have been encouraged to take their own lives or to self-harm[27] and where livestreaming paired with screen recording has been used to spread "hateful footage."[28] The Illegal Harms Code also highlights the risk of grooming posed by hosting livestreams.[29]
- Recommended measures in the Code: There are no specific measures which would robustly mitigate the risk from this functionality and there are no measures relating to age-appropriate access to livestream (e.g. preventing children in certain age groups from watching and/or hosting livestream broadcasts). This is also the case for the Illegal Harms Code.
- Measures which would be required to address this: Depending on the specific risk profile of the service, providers should consider implementing one or more of the following to mitigate risks:
    - Disable the ability to host livestreams for all children or children in certain age groups.
    - Disable livestream features and functionalities (e.g. 'follow', comments, co-hosting, Q&A or gifting) for all children or children in certain age groups.
    - Implement highly effective or effective age assurance commensurate to risk.

[25] Lord Parkinson of Whitley Bay, 19th July 2023, Online Safety Bill, Report Stage (5th Day)

[26] Vol. 3, 7.2.79

[27] Vol. 3, 7.2.82

[28] Vol. 3, 7.4.80

[29] See: Vol. 2, Illegal Harms, p. 47: "Grooming can also often include coercing or manipulating a child into performing sexual acts over livestreams. Perpetrators can also use comments on posted or livestreamed content to build rapport with children, as well as exchange contact details. Livestreaming and commenting on content have therefore also been included in the risk"

- Implement policies to prevent livestreams featuring children in bedrooms, classrooms and bathrooms.
- Implement policies to require adult supervision of children's livestreams.
- Implement policies to restrict viewing access to livestreams where heightened risk from real-time broadcast cannot be managed effectively through moderation.

Direct messaging and 'friend' requests:

- Risk posed by this functionality: Volume 3 includes considerable research of the risk associated with direct messaging, pertaining not just to content-based harms but also to conduct-based harm. This includes cases where a 14-year-old accepted 'friend' requests from people they did not know who sent them pornography and attempted to take them to another platform,[30] evidence of its prolific use by perpetrators of child sexual exploitation and abuse – some of whom pose as 'anorexia coaches' to exploit young women and girls,[31] and how it is commonly used in bullying campaigns.[32] 5Rights has seen videos of children under 8 who have received friend requests from adult strangers.[33] Private messages are often encrypted or subject to heightened restrictions on proactive moderation – this lack of oversight means they are high risk especially when users can send images or videos privately or they are ephemeral (only available for a limited time e.g. disappearing message functions).
- Recommended measures in the Code: Under the Code, children's accounts would still be identifiable to strangers, meaning perpetrators could still add a child user as a 'friend' which would allow them to message children privately and also to share links which take them to other unregulated services. Messages sent to and from children's accounts could still be ephemeral and could include attachments.
- Measures which would be required to address this: Depending on the specific risk profile of the service, providers should consider implementing one or more of the following to mitigate risks:
  - Disable direct messaging for all children or children in certain age groups.
  - Prevent 18+ users from sending unsolicited 'friend' requests to U18s (if this activates access to direct messaging).
  - Disable ephemeral messaging (e.g. 'disappearing' messages) for all children or children in certain age groups.
  - Prevent attachments being sent in private messaging for children or children in certain age groups.
  - Implement effective inference-based moderation systems to identify suspected bad actors and take action to prevent them from contacting children.
  - Provide clear and unambiguous warnings to children when they have been contacted by suspected bad actors.

[30] Vol. 3, 7.1.50
[31] Vol. 3, 7.3.68
[32] Vol. 3, 7.5.62
[33] Available upon request

Ephemeral content (content only available for a limited time e.g. disappearing messages, 'stories', content feeds etc.):

- Risk posed by this functionality: Volume 3 details how ephemeral content, such as 'stories' functions present on many large user-to-user services, have exposed children aged 14-17-years-old to violent and sexual content posted by their connections.[34]
- Recommended measures in the Code: There are no specific measures which would robustly mitigate the risk from this functionality or measures for age-appropriate design (e.g. turning this feature off for certain age groups).
- Measures which would be required to address this: Depending on the specific risk profile of the service, providers should consider disabling ephemeral messaging for all children or children in certain age groups.

Recommender systems

- Risk posed by this functionality: Volume 3 includes considerable evidence of the risk posed by recommender systems, including how algorithms show suicide and self-harm content[35] and eating disorder content[36] to children who have not sought it out. Research which found 7-in-10 teenage boys had seen content promoting misogynistic views via a recommender system.[37] Volume 3 also discusses how children can fall into 'rabbit holes' and filter bubbles where their feeds are filled with harmful content and fewer alternative kinds of content are shown.[38]
- Recommended measures in the Code: There are limited measures which would fully mitigate or manage the risk from recommender systems. While the Code would require the prominence of harmful content in recommender systems to be limited, this would not address cumulative harm in a robust way. For example, these measures would not address harm caused by concentration and volume of PPC, PC, and 'adjacent' content (e.g. high dosage of dieting, juicing, fitness, weight loss journey videos which could cause harm relating to eating disorders with no counternarrative). There are also no measures which would address 'filter bubbles' or 'rabbit holes' (i.e. when the way an algorithm is designed pushes users towards increasingly extreme content) as opposed to just removing PPC or PC.
- Measures which would be required to address this: Depending on the specific risk profile of the service, providers should consider implementing one or more of the following to mitigate risks:

[34] Vol. 3, 7.1.62
[35] Vol. 3, 7.4.15
[36] Vol. 3, 7.3.95
[37] Vol. 3, 7.4.15
[38] Vol. 3, 7.11.50

- Audit the design of algorithms (intentions, inputs, instructions and impact) and carry out testing on AI systems to ensure they are safe and age-appropriate by design and to understand how they perform.
- Identify and address risk of cumulative harm from high doses of PPC, PC and 'adjacent' content.
- Ensure users' ability to give negative feedback about recommender systems includes feedback on cumulative harm.
- Ensure decisions made about exposure to PC, NDC and 'adjacent' content reflect the vulnerabilities and capacities of children in different age groups.
- Disable, 'detoxify' or redesign persuasive design features that extend use and increase risk, such as introducing 'linear' feeds of content or introducing 'timeouts' for child users.

In this draft of the Children's Safety Code, the highest possible protection a child can benefit from is a more protective default setting[39] (of which there are only five) or an enhanced user control setting option (of which there are only three).[40]

This approach over-emphasises the content issues and downgrades the issues of conduct, contact, and contract (that is the design purposes relating to extending time and engagement of users), including those that Ofcom's own research has identified. Not considering features and functionalities ignores Section 12(8) of the Act which states that the child safety duties apply "across all areas of a service" and require service providers to take measures in areas including "the design of functionalities, algorithms and other features."[41]

2. Revise the measures in the Code so that 'Safe Harbour' is only given to services that mitigate and manage all risks identified in Volume 3 (Children's Risk Register)

Whilst we acknowledge that the risk mitigation proposals set out in Volume 5 include cross-cutting measures, for example on governance and terms of service, collectively the 40 measures fail to mitigate risks to children identified in Volume 3.

This is concerning, given that fulfilling these measures allows services to claim 'Safe Harbour.' As currently drafted, the Code would mean Ofcom must consider a service to have met its child safety duties even when children are still at risk of serious harm.

The Code does not fulfil its function as set out in the Schedule 4 of the Act that *"Ofcom must ensure that measures described in codes of practice are compatible with pursuit*

[39] There are only five more protective default settings within the Code which replicate those set out in the Illegal Harms Code of Practice. See: Illegal Harms, Vol. 4, Chapter 18

[40] See: Measures US1-US3

[41] s.12(8)(b), Online Safety Act 2023

of the online safety objectives."[42] This undermines the purpose and expectations the public have of the Act.

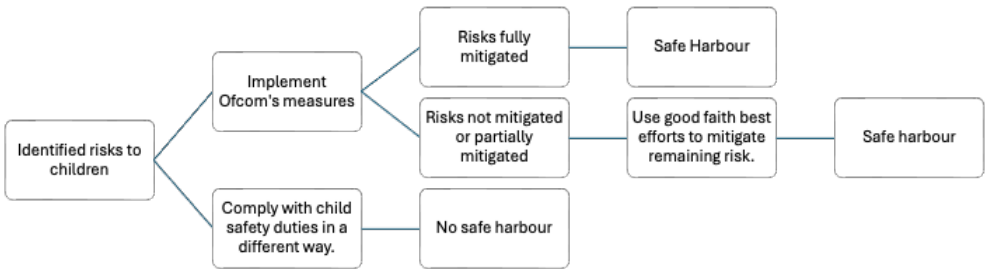
Proposal to amend the 'Safe Harbour' boundary

We acknowledge that there is value in creating a regulatory framework that manages the risk of children's exposure to some of the most egregious content, but this fails to reflect the purpose of the Act, the intention of Parliament or the needs of children and their parents.

We recommend reconstituting the 'Safe Harbour' boundary so that services would only be entitled to claim it if they have:

a. Complied with all the measures in the Code; and
b. Taken steps to address the remaining risk on the service.

This framework would also be adaptable to many different services who will have their own mitigation strategies in place and have very complex design models (see figure below).



3. Require regulated services to give separate consideration to children in different age groups by implementing age-appropriate design (as required under s.11 and s.12 of the Act)

Throughout the child safety sections of the Act, there is a clear expectation that risk to children in different age groups must be identified and addressed separately.[43] This is in acknowledgement of the fact that, as Ofcom correctly notes: "while all children are at risk, harmful content disproportionately affects certain groups."[44] This is also true of

[42] Schedule 4, Online Safety Act 2023
[43] See: s.12(2)(a), Online Safety Act 2023: "A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to effectively… mitigate and manage the risks of harm to children in different age groups"
[44] Vol. 3, 6.6

features and functionalities and Ofcom provides in detail in Volume 3 about how risk manifests in different age groups.[45]

Despite this clear direction from the Act, and extensive evidence of how different age groups experience risk,[46] the Code has no requirement to assign children who are old enough (typically 13-17-years-old) to age-appropriate experiences.[47] Instead, Ofcom has chosen to focus only on protecting all children from 18+ content harms.[48] This does not meet the purposes or text of the Act, or children's needs. It also falls below current best practices, where several regulated companies incorporate at least some aspects of age-appropriate design into their wider safety strategy. Research into how tech companies have responded to the Age Appropriate Design Code[49] points to a number of changes that have been made to make the services age-appropriate:

TikTok has put in place a curfew which means 13-15-year-old users to do not receive notifications after 9pm, whereas 16-17-year-olds do not receive them after 10pm.[50] It has also disabled access to direct messaging for under 16s and does not allow users (irrespective of age) to send images or videos privately and children cannot host livestreams.[51]

Roblox distinguishes between users under 13 and those 13 and older to provide different experiences. Posts and chats are filtered for inappropriate content and to prevent personal information from being posted if they are under 13, whereas users 13 and older have the ability to say more words and phrases.[52]

Microsoft Edge provides different settings in its Kids Mode depending on if children are between 5-8-years old, or 9-12-years-old.[53]

[45] See: Vol. 3, 7.1.22: "A study found that of the young adults (18-21-year-olds) who reported having previously watched online pornography, those reported first watching it at age 11 or younger were significantly more likely to score lower on self-esteem than those who reported having first watched it at age 12 or older"

[46] See: Vol 3, 7.15

[47] Vol. 5, 15.319: "Given these limitations, our proposals focus at this stage on establishing recommended protections for all children under the age of 18, rather than tailoring those protections for children in different age groups"

[48] Vol. 5, 15.317: "We recognise that age is a key factor that will affect children's expectations and experiences of being online and our research indicates that certain online behaviours vary by age and developmental stage. However, there is currently limited evidence on the specific impact of harms to children in different age groups"

[49] Children and Screens (2024) *UK Age Appropriate Design Code: Impact Assessment* p.9; See also: Wood, S. (2024) *Impact of regulation on children's digital lives,* Digital Futures for Children, 5Rights Foundation, LSE

[50] TikTok (ND) *Teen privacy and safety settings*

[51] TikTok (ND) *Terms of Service,* 4.4

[52] Roblox (ND) *Safety Features: Chat, Privacy & Filtering*

[53] See: Microsoft (ND) *Learn more about Kids Mode in Microsoft Edge*

Xbox allows for filtering of content to meet the ages of children based on PEGI content ratings – PEGI 3, PEGI 7, PEGI 12, PEGI 16 and PEGI 18.[54] Children can request access to content which parents can approve or deny.

Pinterest makes all accounts under 16 private and the 'boards' and 'Pins' they make will only be visible to them by default. Under 16 accounts can only exchange messages with mutual followers.[55]

To be safe and age appropriate by design, a service must make and publish decisions about how old children must be to use the service; which content, features and functionalities the service considers age-appropriate for children in different age groups and what additional settings, controls and support it has put in place for children in those age groups. Child development theory is well-established,[56] and children have a right to be treated according to their evolving capacity.[57] No parent or child would consider that it is appropriate to give all children under 18 the same experience.

For example, sex education or understanding the dangers of driving may be hugely necessary for a 16 or 17-year-old, but that same information in the hands of a 7-year-old may be frightening. Similarly, it may be age-appropriate for a 15-year-old to upload videos to YouTube but not age-appropriate to be seen livestreaming in their bedroom to millions of followers. It may also be the case that both of those situations may not be age appropriate for a 10 or 12-year-old. The current iteration of the Code treats these scenarios and all others the same whether aged 4, 14 or 17.

4. Require regulated services to set and enforce minimum age requirements

Volume 5 states that the Code will not require services to identify and remove underage users from its services, even where a provider has deemed their service unsuitable for young children:

> "In developing our proposed measures, we considered whether it would be appropriate and proportionate to recommend that services that state a minimum age in their terms of service should use effective measures to enforce that provision, for instance, highly effective age assurance. We determined that this would not be proportionate."[58]

---

[54] Microsoft/Xbox (ND) *Family-friendly gaming for everyone*. See also: Pan European Game Information (2017) *What do the labels mean?*

[55] Pinterest (ND) *Teen safety options*

[56] See: 5Rights Foundation (2023) *Digital Childhood: Addressing childhood development milestones in the digital environment*

[57] As required by: United Nations Committee on the Rights of the Child (2021) General comment No. 25 on children's rights in relation to the digital environment, s.IV

[58] Vol. 5, 15.314

This determination effectively means that under the Code age assurance can only be a technology that provides exact age (under or over 18) through facial age recognition or a hard identifier (official document).[59] This is a regressive and binary view of age assurance.

'Highly effective' age verification which provides users exact age as described in the Code is only one level of age assurance. It is imperative that Ofcom considers the wider ecosystem of age assurance methods which, while not 100% effective at verifying an exact age, can separately or (more often) collectively achieve a greater level of certainty about the age of users and enhance service providers' ability to give children age-appropriate experiences. Many services already adopt some effective age assurance processes outside of age verification as part of their safety strategies, for example:

- AI models to detect suspected underage users.
- Making it possible for users and non-users to report underage users (e.g. via a reporting button).
- Designing self-verification (tick box) in line with best practices standards (e.g. no nudge toward 'correct' age and preventing users from trying again if they say they're too young).
- Training moderators to consider whether accounts they are reviewing may be held by underage users and create a mechanism for human review.
- Using keyword detection (e.g. "I am in Year 6") in their automated moderation strategy.

Ofcom's failure to recommend any of the current strategies used by service providers, despite setting out where these are currently in use Volume 5,[60] means the Code will not lead to a levelling-up and/or standardisation of current practices.[61] [62]

The proposals demonstrate a missed opportunity to broaden thinking on age assurance beyond hard identifiers, such as the potential for using age tokens which can provide the age of user while minimising the need for personal data.[63] Irrespective of whether a service uses age assurance or age verification, or both in combination, a foundational principle of data protection is data minimisation and we would urge Ofcom to consider the ICO's guidance on how this can be achieved in age assurance strategies.[64]

---

[59] It has also decided that age assurance should only be used to enforce 18+ restrictions on content (on services that do not prohibit the content under their terms and conditions). See: Vol. 5, 15.133 (Measure AA3) & Vol. 5, 15.164 (Measure AA4)

[60] Vol. 5, 15.28-15.38

[61] Whilst current standards are considered entirely insufficient to prevent widespread underage access to online services, they have made a contribution. For example, between January-March 2024, TikTok removed 21,639,414 suspected underage users globally. See: TikTok (2024) *Community Guidelines Enforcement Report*

[62] We would urge Ofcom to consider insight from Arturo Bejar, former Director of Engineering at Facebook who has argued that tech companies already develop systems to detect and remove under 13s from services, and his concern that some companies have misrepresented what it is possible to do. See: Family Online Safety Institute (2024) *FOSI 2024 European Forum - Fireside Chat: Lessons from a Facebook Whistleblower,* 34:52-38:13

[63] 5Rights Foundation (2021) *But how do they know it is a child? Age Assurance in the Digital World*, pp. 38-39

[64] See: Information Commissioner's Office (ND) *GDPR Principle (c): Data minimisation*

Outside of proactive age assurance efforts, 5Rights research[65] has found tech companies serve age-relevant targeted advertising to children as a core feature of their business model, demonstrating that they already know which users are children. If services already know where underage children are, they must be held accountable if they do not use this information to remove them.

Ofcom has said that minimum age requirements will be enforced through provisions requiring services to uphold their Terms of Service, but the Online Safety Act does not require regulated services to state a minimum age requirement or to provide details of what content, features and functionalities are limited for children or children in certain age groups. Therefore, if a service provider chooses not to include this information in its Terms of Service (and the Code creates strong incentives for them not to do so, or to include it as a recommended minimum age rather than a policy), Ofcom has no powers to take action against them.

It is the expectation of the public that companies will face enforcement action for routinely allowing children under 13s access to services and products that service providers themselves have said are not suitable for those children. The appropriate place to set these rules is within the Children's Code.

5. Require Ofcom to fully identify the limits of its regulatory powers that prevent it creating a comprehensive Code. To the extent that its powers are insufficient to fulfil any aspect of the Act, Ofcom must report this to the Government.

Schedule 4 of the Act (Codes of Practice) states "the measures described in the code of practice must be sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice.[66]

Ofcom has interpreted this to mean that only measures that have been tried and tested by industry can be used. This omits safety measures that regulated companies have not been willing to try and leaves a significant gap between risk and mitigation. This is troubling given the current provisions on 'Safe Harbour' (see above).

Ofcom should seek and publish a Legal Opinion on whether:

(a) It is able to require measures where the evidence base is incomplete but there are reasonable grounds to believe it would be effective;

(b) Whether measures that are outcomes-based can meet the clarity requirement in Schedule 4; and

[65] 5Rights Foundation (2021) *Pathways: How digital design puts children at risk*, p. 84

[66] See: Schedule 4, 2(b), Online Safety Act 2023

(c) Whether, in the absence of a reasonable measure, Ofcom must require the risk (feature, functionality, or content) to be disabled until a measure can be found.

If the Opinion supports a wider interpretation of measures, Ofcom should immediately review the measures proposed in the Child Safety Duties Code of Practice to include measures that will deliver on the overarching duty to ensure that services are made safe by design and children are given a higher level of safety than adults.[67] If the Opinion confirms Ofcom's current interpretation of the Act, the Government should immediately amend the Act so that measures result in material protection to children by design and default.

It is also Ofcom's position that it cannot make substantive changes in response to the consultation unless it reconsults. This is out of step with other regulators[68] and undermines the purpose of a consultation.

Sections 41 and 43 of the Act set out the process Ofcom must go through to issue Codes of Practice. Neither section contains any provision that would require Ofcom to carry out further consultation on changes made in response to the consultation before submitting the draft to the Secretary of State.

Legal Opinion should be sought on the level of discretion Ofcom has to change the Code following consultation. If the advice is that it can make changes, it should do so and communicate what those changes are and why it made them. If Legal Opinion determines that consultation cannot result in changes from Ofcom, this must be reported to the Government and the Act amended. The Legal Opinion (or a summary) should be published.

[67] s.1, Online Safety Act 2023

[68] Information Commissioner's Office (2024) *ICO Consultation Policy* states "in some circumstances it may be necessary for us to conduct a follow-on consultation, or to reconsult on an issue. However, we will seek to minimise these occurrences"