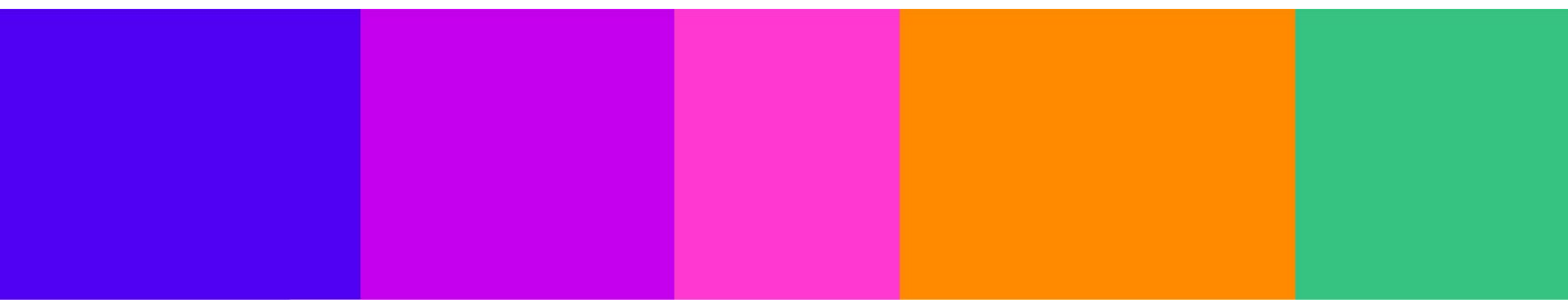# Consultation response form

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

Consultation title	Consultation: Protecting children from harms online
Organisation name	Office of the Victims' Commissioner for England and Wales

Your response

Question	Your response
Volume 3: The causes and impacts of online harm to children. **Draft Children's Register of Risk (Section 7)** **Draft Guidance on Content Harmful to Children (Section 8)**	

Confidential? – N

4. Do you have any views on Ofcom's assessment of the causes and impacts of online harms? Please provide evidence to support your answer.

5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer.

7.1 Pornographic Content

Pornography is now freely and easily accessible to anybody who can access the internet, including, as has been well explored in public discourse and by policy makers, children. Pornography exposure is widespread and normalised – to the extent that children cannot 'opt-out'. Research by the Children's Commissioner found that 64% of children interviewed had seen porn.[1] The average age at which children first see pornography is 13. By age nine, 10% had seen pornography, 27% had seen it by age 11 and half of children who had seen pornography had seen it by age 13.[2] This research also found that young people were most likely to have seen pornography on X, a mainstream platform, rather than a dedicated pornography site.

Research shows that online mainstream pornography is "overwhelmingly centred on acts of violence and degradation towards women."[3] A government literature review which considered the academic research in this area found that:

> 'There is substantial evidence of an association between the use of pornography and harmful sexual attitudes and behaviours towards women. The nature and strength of this relationship varies across the literature, and there are many potential moderating (potentially even mediating) variables that require further investigation. However, it is clear that a relationship does exist, and this is especially true for the use of violent pornography.'[4]

The same review argues that, while it cannot be said that there is a direct causal link, pornography use is a factor, amongst other potential factors, that appears to contribute to a permissive and

---

[1] Young people and pornography | Children's Commissioner for England
[2] Ibid
[3] Sun, C., Bridges, A., Johnson, J. & Ezzell, M. (2014). Pornography and the Male Sexual Script: An Analysis of Consumption and Sexual Relations. *Archives of Sexual Behavior*, 45(4).
[4] The relationship between pornography use and harmful sexual attitudes and behaviours: A literature review prepared by The Behavioural Architects (Joanne Upton, Alya Hazell, Rachel Abbott and Kate Pilling) for the Government Equalities Office (2020) (publishing.service.gov.uk)

Question	Your response

conducive context that allows harmful sexual attitudes and behaviours to exist against women and girls.[5]

7.1.25 – 7.1.29: The Register of Risks discusses the relationship between exposure to pornographic content and harmful sexual behaviours, and the normalisation of sexual aggression. It might be useful for this section to have some named examples of harmful sexual behaviours, or to explicitly state what is meant by this. Understanding of "harmful sexual behaviour" is likely to vary significantly and be highly subjective some providers may interpret this as only being illegal sexual behaviour e.g. rape, and therefore only take action which seeks to moderate content containing explicitly illegal material, rather than considering wider societal harms.

Additionally, there is no reference to the long-term impact that exposure to pornographic content and the normalisation of sexual aggression can have on interpersonal relationships and the prevalence of domestic abuse.

In 2020, BBC Disclosure and BBC Radio 5 Live commissioned a survey of 2,049 men in the UK aged 18 to 39 to assess the prevalence of so-called "rough sex". Seventy-one per cent of the men who took part said they had slapped, choked, gagged or spat on their partner during consensual sex. Of those who had engaged in such activity, about one third said they would not obtain consent for the activity either before or during sex. Importantly, around 60% of those who did engage in this type of activity agreed that porn had influenced them.[6]

The Children's Commissioner also found that frequent users of porn are more likely to engage in physically aggressive acts. The research also found that young people are frequently exposed to violent pornography, depicting coercive, degrading or pain-inducing sex acts; 79% had encountered violent pornography before the age of 18.[7]

This is important as there is evidence, from a longitudinal study carried out into the effects of early exposure to pornography, that "early exposure for males predicted less progressive gender role attitudes, more permissive sexual norms, sexual harassment perpetration".[8] There are clear links between the prevalence of domestic abuse and violence against women and girls, and exposure to violent and extreme pornography, and the Register of Risks fails to explicitly recognise these, missing a crucial opportunity to promote the need for better understanding of these themes amongst internet service providers.

This chapter deals with pornographic content which is designated under the Online Safety Act as priority primary content which is harmful to children, but which is not illegal in its own right. 7.1.5 references the fact that some of the pornographic content encountered by children online is illegal, but that illegal types of pornography is addressed by the 'Tackling Illegal Harms' guidance. We would advise that the Register and Guidance for the Protection of Children should not assume that the legislative provisions within the Online Safety Act and the guidance on 'Tackling Illegal

[5] Ibid
[6] 'I thought he was going to tear chunks out of my skin' - BBC News
[7] 'A lot of it is actually just abuse': Young people and pornography - Children's Commissioner for England and Wales, 2023
[8] X-Rated: Sexual Attitudes and Behaviors Associated With U.S. Early Adolescents' Exposure to Sexually Explicit Media - Jane D. Brown, Kelly L. L'Engle, 2009 (sagepub.com)

Question	Your response

Harms' are watertight frameworks for effective regulation. Guidance aimed specifically at protecting children must also address the specific impacts of exposure to illegal pornographic content on children, as there is ample evidence of their exposure to this content, particularly self-generated CSAM. For further evidence on why existing legislation and regulation cannot be relied upon to act completely effectively, and why this guidance cannot make the assumption that it can, please see the Victims' Commissioner's submissions to the [Illegal Harms consultation](#) and the [Independent Inquiry into Pornography Regulation, Legislation and Enforcement](#).

7.1.8 states that 'some of the evidence in this section may relate to content that is broader than the definition of pornographic content in the Act or set out in the draft Guidance on Content Harmful to Children'. This is good and should be encouraged. It is vital that there is significant consideration given to and engagement with wider societal harms, particularly relating to violence against women and girls, and how they are exacerbated by children's exposure to pornographic content.

7.4 Abuse and Hate Content

The definition of abuse and hate content used by Ofcom is intrinsically linked to the definition of a hate crime, due to the specific link made with listed characteristics. It is important that this definition is extended to make clear that it is not limited to abuse in relation to hate crimes. Abuse and hate content can be directed at anyone and can be based on information about the victim known to the abuser which does not relate to a listed characteristic. For example, under the current definition set out by Ofcom, a comment directed towards a victim of rape speaking out about her experience, stating that she deserved what happened to her, would not fall under the definition of abuse and hate content as it does not specifically relate to a listed characteristic (despite rape being a gendered crime). This is despite the high harm to the victim which would obviously result from reading such a comment. This needs to be taken into account when considering how to define and identify abuse and hate content.

In addition, more detail should be given, preferably with specific and tangible examples, about how abuse and hateful content can manifest online. 7.4.11 states that it can 'take many forms, including misogyny, racism, transphobia, homophobia and ableism', but misogyny is the only one which receives any kind of detail, which is still limited. It is good that there is reference to the need to consider intersecting influence of demographic risk factors (7.4.35) but there should be more detail on this, with specific reference to higher risk intersections e.g. misogynoir. Whilst it is important that the guidance does not set out so much detail that it allows service providers to exclude any content which isn't detailed, the current vagueness lacks nuance and an explanation of how different forms of abuse and hateful content can manifest both in isolation and cumulatively.

For example, 7.4.16 states that online harassment was reported as more common than street harassment. Yet there is no detail given about what online harassment looks like, or how to identify it. This is particularly concerning given what we know about poor law enforcement responses to course of conduct offences like harassment and stalking. Research commissioned by the Victims' Commissioner in 2022 found that victims of cyberstalking were significantly less likely to feel the police treated them with respect compared to victims of other online harms, with many saying that they did not feel that police were adequately trained to understand the nature of online

Question	Your response

abuse and its implications. Only 10% of cyber stalking victims felt their accusations were thoroughly investigated and almost half of the victims of this offence, 45% were told to remove themselves from social media.[9]

Here, we would also like to reference the NPCC and College of Policing's Violence Against Women and Girls National Policing Statement 2024. This report, which outlines the scale of violence against women and girls, sets out the evolving threat posed by online abuse and the risk of over-reliance on criminal justice responses.

> *The threat of online abuse is expected to continue to change rapidly, not least due to the rise of Artificial Intelligence (AI). Ofcom (2023) found that children and teenagers are more likely to have embraced generative AI, with 79% of teenager respondents aged between 13 and 17 had already experimented with this technology.*

> *It is also highly likely that implementation of the Online Safety Act 2023 will increase the demands on and expectations of policing to identify and tackle online and tech-enabled VAWG. As it stands, over 50% of the public do not currently think that the police have enough resources to deal with online offences.*

> *We cannot provide the appropriate solution to either control or regulate people's safe use of online platforms and technology. It is our view that to address this evolving threat more timely robust action is required from government to improve the response by the industry.[10]*

7.4.24 recognises that encountering this content can result in children withdrawing online, effectively self-censoring themselves. It would be good for the guidance to explicitly recognise the disproportionate impact this has on certain targeted groups, and how their self-removal from online spaces exacerbates the problem by creating an echo chamber for hateful content, leading to this content being disproportionately amplified in relation to the number of people actually holding these views.[11]

7.4.38 – 7.4.45 deals with "gender" as a user demographic base risk factor. In this section, it would be helpful to address the fact that exposure to hateful/misogynistic content can normalise such attitudes amongst young women and girls. Currently, the guidance seems to only deal with the impact of altered attitudes on young men and boys, suggesting that girls only suffer from an emotional impact or a censorship impact. In fact, as research shows, some girls may internalise misogyny which increases their risk of accepting of harmful behaviours.[12] Here it would be helpful to make a direct link to domestic abuse and/or violence against women and girls, and to explicitly recognise the link between online and offline offending. It would also be good to name some specific examples of how these harmful attitudes can manifest, e.g. gaslighting.

[9] The Impact of Online Abuse: Hearing the Victims' Voice - Victims Commissioner (victimscommissioner.org.uk)
[10] National Policing Statement 2024 For Violence Against Women and Girls (VAWG) - NPCC and College of Policing
[11] The Self-Censoring Majority: How Political Identity and Ideology Impacts Willingness to Self-Censor and Fear of Isolation in the United States - Alycia Burnett, Devin Knighton, Christopher Wilson, 2022 (sagepub.com)
[12] Women's Aid publishes groundbreaking research looking at what influences children and young people's understanding of domestic abuse - Women's Aid (womensaid.org.uk)

Question	Your response

Following on from this, whilst it is welcome that the guidance references the misogynistic content being encountered by children and ties to the 'manosphere', it is frustrating that there is not a separate chapter devoted to the risk posed to children by online misogyny. Recognition of online misogyny as a separate high-risk harm is crucial given its prevalence and relationship to multiple harms currently explored in the Register of Risk, including violent content and pornographic content.

Gender identity and sexuality are grouped as risk demographic factors (7.4.46 – 7.4.50), however these are arguably distinct from each other, particularly in the modern online landscape where trans-exclusionary groups promote content which argues that trans rights and lesbian, gay and bisexual rights are conflicting.[13][14] This criticism could also be applied to other demographic factors, where there are unhelpful groupings which don't recognise the distinct experiences of different groups, e.g., ethnic identities. Whilst we understand that some groupings are necessary for ease, such groupings assume some degree of homogeneity, whereas it is vital to recognise the nuances and heterogeneity within groups and experiences.

It may be helpful for the guidance to include a point about the need to be sensitive to 'spikes' in abusive content, in response to global events. For example, anti-Asian content became more prevalent during the Covid pandemic due to hateful rhetoric labelling Covid as 'the Chinese virus'.[15] The guidance should include reference to these spikes, with reference to the fact that they can result in a higher volume of 'lower level' abusive content which may not be serious enough in isolation to get flagged up, but when viewed as part of a cumulative campaign of abuse would constitute high harm.

7.4.90 – 7.4.93 deals with recommender systems and highlights the limitations of users to fully control the content on their feeds. This section demonstrates the need for greater regulation on the ability of providers to design algorithms and content recommender systems which allow for the promotion of harmful content, even when the user hasn't 'liked' or searched for any of this kind of content proactively. There is currently an implicit acceptance that this is a fact and has to be adapted to, whereas the reality is there should be much more onus on service providers to address this.

There is a wider issue here, relating to the absence of 'safety by design' and the piecemeal approach taken towards recommender systems. Ofcom states that "the functionalities and characteristics [of recommender systems] we describe as risky are not inherently harmful and can have important benefits." While this is true, there are issues with the way companies are being asked to mitigate the risks of these systems. The onus is placed far too much on regulation of content after it has been created and limiting children's risk of being recommended this content, rather than putting appropriate safeguards in place to reduce the risk of this content being present in the first place. There are also issues with the business model which is referred to in the risk assessment and risk profiles, particularly around the financial incentives associated with the promotion

---

[13] LGB Alliance: Anti-trans lobby group's troubling, ugly history (thepinknews.com)
[14] Gender Recognition Act Reform - LGB Alliance UK (lgballiance.org.uk)
[15] Association of "#covid19" Versus "#chinesevirus" With Anti-Asian Sentiments on Twitter: March 9–23, 2020 | AJPH | Vol. 111 Issue 5 (aphapublications.org)

Question	Your response

and creation of hateful content which is designed to provoke a reaction and generate 'clickbait'. This is not addressed in the measures.

<u>7.6 Violent Content</u>

It is welcome that there is substantial recognition of the links between exposure to online violent content and manifestation of offline violent acts. It is also welcome that normalisation and desensitisation towards this kind of content is discussed at length. 7.6.21 states that older children aged 16-17 believe they are becoming desensitised to violent content and may not be able to acknowledge the impact on them of consuming violent content. However, exposure to violent content online can be related to a number of psychological and behavioural outcomes. It is vital that the guidance explicitly makes clear that children and young people's perceptions of the impact of exposure to violence content on them does not necessarily directly match with the actual long-term impact on them.

We recommend that there should be more discussion of the variety of violent content experienced, and the impacts felt, between different age groups. 7.6.34 – 7.6.36 deals with age as a user demographic risk factor and addresses the differing risks of harm from violent content, and the effect of exposure to it, for different age groups. Yet, there is no discussion of what violent content is being most commonly encountered by different age groups, and how this manifests.

We recommend that there should be more read-across some of the examples given in Section 8. It is welcome that sexual violence and domestic abuse are listed as examples of content that encourages, promotes, or provides instructions for an act of serious violence against a person, although detailed examples would be a useful improvement. However, there should also be recognition of how sexual, gendered violence can manifest in other forms of violent content, in particular gaming content which falls within *Table 8.8.3: Description and examples of content that depicts real or realistic serious violence against a person, or the serious injury of a person in graphic detail.* This is due to the prevalence of misogynistic violent content in video games such as Grand Theft Auto and Call of Duty which children are not legally allowed to buy or own but which many do, as set out in the Register of Risks (7.6.55).

Following on from this, gaming services are highlighted as an example of services where young people can be exposed to violent content, and there is recognition that risks can emerge when violent gaming content is encountered by children younger than the target audience of the game. This section should explicitly discuss the types of violent content experienced, in particular making an explicit link between the prevalence of violence against women and girls in certain games such as Grand Theft Auto and the normalisation of violent attitudes towards women and girls amongst young men and boys.

We would also encourage you to include more detail in both the Register of Risks and Guidance dealing with violent content when discussing how exposure to violent content can lead to normalisation and acceptance of violence against women and girls and domestic abuse. In particular, there should be explicit inclusion and naming of domestic abuse-related examples of psychological violence, such as gaslighting which minimises violence and coercive and controlling behaviour. Whilst section 7.6.25 mentions the links between exposure to content promoting VAWG and 'a difference in attitudes towards violence among children', the section does not delve specifically into what those attitude shifts mean for women and does not touch on the wider societal impacts

Question	Your response

in relation to violence against women and girls and domestic abuse. It would be encouraging to see Ofcom recognise how this exposure could affect romantic or familial relationships, and how increased risk and normalisation of violent behaviour in society is likely to result in higher prevalence of domestic abuse.

It is noted that the ability to forward, share, and therefore 'promote' violent content has a harmful effect because it creates a sense of normality. This is an observation that can, and should, be applied to multiple harms.

6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer.

We have a limited evidence base to be able to provide in-depth answers to questions focusing on assessment of risk by age. However, we would like to bring Ofcom's attention to some overarching issues:

- The age assessment groupings for younger children makes a number of assumptions regarding levels of parental supervision and parental controls. One assumption is that parents will have sufficient levels of understanding of the various technologies and service providers that their children are interacting with to provide appropriate supervision. The guidance should start from an assumption that all parents are non-internet users, to take full account of the range of understanding held by parents of the services their children are using. Additionally, this assumption does not take into account differences in the types of parental controls and restrictions in place across different service providers. There needs to be more in the guidance to support parental understanding of the different restrictions and controls available on different websites.
- If Ofcom continues to assume that parents and teachers will be the first port of call for regulation of their children's internet access, this must be supported by robust RHSE guidance. The RHSE guidance published by the last government is inadequate for safeguarding children whom the 'protection of children' guidance is aimed at. Whilst it is likely that the new government will revisit and possibly re-draft this guidance, it is vital that Ofcom considers the interdependencies between this guidance and its own regulation. Ofcom's own guidance recognises that 10% of children have been exposed to pornography by the age of 9 and that this rose to 51% of children aged 11-13. Yet the RHSE guidance prohibits teachers from educating children of this age around sex education other than in the context of conception and birth as part of the science curriculum, stating that "the risks of inappropriate online content can be discussed in an age-appropriate way from year 7, however, the details of sexual acts should not be discussed before year 9." It is widely recognised, and discussed in this submission, that exposure to pornography can affect children's views of what is normal and acceptable sexual activity, and the RHSE guidance's failure to recognise this means that children will be more vulnerable to the influence of harmful content. Whilst the RHSE guidance is obviously out of scope for Ofcom, it is crucial that Ofcom do not rely on an assumption that this guidance is adequate for enabling teachers and parents to protect children from harmful online content.

Volume 5 – What should services do to mitigate the risk of online harms

Our proposals for the Children's Safety Codes (Section 13)

Question	Your response

Confidential? – N

The proposals set out in Volume 5 fall outside the scope of the Victims' Commissioner's work; therefore, we are unable to offer any original evidence relating to this part of the consultation. However, we would like to signpost towards the responses submitted by the Children's Commissioner and the Online Safety Act Network (OSAN), in particular echoing the concerns raised by OSAN regarding the effectiveness of age assurance measures. For ease, some of the most pertinent points are quoted here:

- The implementation of age assurance measures is not a fundamental "safety-by-design" measure. For services that are fundamentally harmful - eg their content is entirely inappropriate for children and under-18s - this is right. For others, the requirement builds in safety to the architecture of the service through age gating - either in its entirety or in part, based on the types of content it serves - but the service that sits behind the age-gating may not intrinsically be made any safer.
- The alignment of the approach taken by Ofcom on governance, risk assessment and (most of) the measures in the codes of practice between the illegal harms consultation and the children's consultation bears this out. Therefore, there is potentially an incentive for services that *could* make themselves safer to decide not to bother with the extra costs that might be incurred and just bar children from accessing their sites.
- Ofcom has not attempted to introduce measures that would take into consideration the different age groups of children who might be on platforms and how harm manifests itself according to age, although some of this is described in the risk register. Ofcom says that this is difficult, though it would seem that the bigger platforms are already very well aware of the ages of children on their platforms to a fairly precise degree of accuracy. See Arturo Bejar from 36 mins here [FOSI 2024 European Forum - Fireside Chat: Lessons From a Facebook Whistleblower (youtube.com)](#) where he mentions "talking to regulators in the UK" and being aware that: "Social media companies .. particularly Meta .. misrepresent what they are able to do. For example, they talked about their inability to detect under-13 accounts … It's not that hard to find an account that an 8-year-old makes. These are all problems that are solvable." If platforms know the age of their users, it should be possible for them to introduce different measures for those different users. It appears here - as Bejar suggests - that Ofcom is taking at face value platforms describing what they are doing now, without looking at what the capacity of age-verification might be - if properly applied, as required under the Act.
- There is a flaw too in using age gating as the means to prevent harm in otherwise anodyne or relatively risk-free environments. If, for example, the service is a small gaming platform that might have instances of severe harm but not in large quantity or on a large scale, then its requirements under the age assurance duties will mean that those instances of severe harm will not get addressed. Eg Volume 4, 12.50: "However, for the avoidance of doubt, we expect that any service with more than 1 million (or between 100,000 and 1 million) monthly UK child users would need a range of robust evidence to demonstrate that it does not in fact pose high (or medium) risk of harm to children in respect of a given kind of content."

Question	Your response
	• Related to this, an obligation/dependency on age verification potentially means that the quality of the service providers' risk assessments is secondary - eg if children aren't on the platform, then they don't need to keep monitoring risks. • There is also the question as to what happens if the percentage of content that is "principal purpose" is just below the threshold designated for age assurance measures to prevent children's access. • With regard to the principles-based approach, we noted that Ofcom does not provide sufficient criteria by which it will measure those outcomes and/or the providers' compliance with their duties. Ofcom put forward arguments about the "nascent" age verification industry (see above, though we also note age verification in some form or other has been required under the Communications Act for more than a decade) which they said justify not having an output level score (especially in relation to technical accuracy). There is a difference between recommending a particular tool (which Ofcom in our opinion rightly is not doing, both in the part 5 guidance and these proposals) and measuring effectiveness of any tool. If the concern is that any one tool could not be effective enough, techniques could be used in combination with other tools. Ofcom's narrow approach means that it is precluding the potential effectiveness of combinations of techniques that might lead to the same outcome.

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