Nexus

Breaking the Cycle of Sexual Abuse
and Abusive Relationships

Consultation Response:

Ofcom Protecting Children from Harms Online Consultation

July 2024

Introduction

Nexus has almost 40 years' experience offering a specialised professional counselling service to people impacted by sexual abuse and abusive relationships. We can provide support to anyone impacted by sexual abuse from age 4 and upwards, availability of children's counselling depends on available funding. We currently also provide support services to adults who are age 18+, identify as male, and who have been impacted by abusive relationships (domestic abuse) as an adult or child. Our Early Intervention and Prevention Training team provide a range of bespoke training and workshops that are available to schools, workplaces, volunteer groups, higher education institutions, individual practitioners, community groups, sports teams, voluntary and charity groups, and businesses.

As providers of Relationship and Sexuality Education as well as a therapeutic intervention service for young people impacted by sexual abuse and abusive relationships, Nexus welcomes this robust, well-evidenced volume of proposals from Ofcom to strengthen protections and accountability measures for online services. As society continues to spend large quantities of time online or on social media, we strongly believe in the responsibility of service providers, government, and strategic stakeholders to protect our children and young people from harms online.

The following comments, suggestions, and questions are based on our expertise and experience supporting children, young people, and their families and carers through therapeutic interventions across Northern Ireland.

Background (Volume 1)

As part of the commissioning and implementation of the Online Safety Act (2023), Ofcom was named as the independent regulator of Online Safety. In this role, Ofcom must set out the guidance, framework, and steps for service providers to take to fulfil their legal duties as set out in the Online Safety Act. Ofcom will also possess enforcement powers to ensure providers' compliance with the agreed safety frameworks and codes of practise. Ofcom has created a 3 Phase approach to implementing the Online Safety Act, described as follows:

Phase One: Illegal Harms Duties - November 2023 to Autumn 2024

- Analysis of the causes and impacts of online harm, to support services in carrying out their risk assessments;
- Draft guidance on a recommended process for assessing risk;
- Draft codes of practice, setting out what services can do to mitigate the risk of harm; and
- Draft guidelines on Ofcom's approach to enforcement.

Phase Two: Child Safety, Pornography, and the Protection of Women and Girls - December 2023 to Spring 2025

- Draft guidance on age assurance for online pornography services
- Draft codes of practise for protection of children
- analysis of the causes and impacts of online harm to children; and
- Draft risk assessment guidance focusing on children's harms.
- Draft Guidance on Protecting women and girls

Phase Three: Transparency, User Empowerment, and other duties on categorised services

- Produce a register of categorised services by the end of 2024
- Publish draft proposals regarding the additional duties on these services in early 2025; and
- Issue transparency notices in mid 2025

Background (Volume 1) continued

This consultation focuses on Ofcom’s proposals for how internet services that enable the sharing of user-generated content ('user-to-user services') and search services should approach their new duties relating to content that is harmful to children.

In this consultation, Ofcom cover:

- How to assess if your service is likely to be accessed by children;
- The causes and impacts of harms to children;
- How services should assess and mitigate the risks of harms to children.

Volume 2: Identifying the Services that Children are Using

A children's access assessment is a process that all Part 3 services in scope of the Act must carry out to determine whether they are likely to be accessed by children. Services likely to be accessed by children must comply with the children's risk assessment duties and children's safety duties.

Volume 2 sets out Ofcom's approach to the Draft Children's Access Assessment Guidance, including age assurance technologies, the meaning of "significant number of children" and how Ofcom proposes services assess whether they are likely to attract a significant number of children.

Nexus Response

We agree with the proposals in Volume 2. As detailed in our response to the Ofcom 'Guidance for Service Providers Publishing Pornographic Content' consultation, it is vital that the age assurance technology is accurate at determining the age of a user, is bespoke for the service type, and should be constantly tested for accuracy and reliability. The Digital Trust and Safety Partnership published Guiding Principles and Best Practises for Age Assurance Methods, detailing the importance of identifying, evaluating, and adjusting for risks to youth to inform proportionate age assurance methods, conducting layered enforcement options, and ensuring that the technology is accessibly, risk-appropriate, and effective.

Regarding Ofcom's approach to the child user condition, we agree that the use of the phrase "significant number of users who are children" should be interpreted not as a flat numerical number, but instead as contextualised by the service itself and the risk of harm to child users.

As Ofcom's own research shows, the top shows for children in 2022 were Squid Game, a series about financially burdened people who participate in deadly children's games for the chance to win money, You, a thriller that follows a man who stalks his partners and eventually murders them, and Grey's Anatomy, a medical drama that includes themes such as abuse, violence, and sexual content. What this research shows is that children are accessing content that can be classified as a risk of harm to their wellbeing but is not necessarily advertised for a child audience. This case study supports Ofcom's interpretation of "significant number of children" in order to ensure that potentially risky services are not ruling themselves out on the children's risk assessment.

The proposed process for children's access assessments is rigorous and intentionally wide-ranging to capture all aspects of service provision, business practises, and child user activity. As Ofcom notes in Section 4, children are also likely to access content, services, and platforms that are not specifically targeted towards their age demographic. By recommending to services to apply the second criterion first in their children's risk assessments, services will be much more likely to be equipped to identify significant child user engagement.

Volume 3: The Causes and Impacts of Harms to Children

Volume 3 presents Ofcom's draft Children's Register of Risks as part of Ofcom's duty to assess the risk of harm to children from content online. The draft Guidance on Content Harmful to Children complements the Register of Risks, providing examples of what Ofcom considers to be, or not to be, content harmful to children.

From Volume 3: "Twelve kinds of content that is harmful to children ('harmful content') are defined in the Act. The Act further groups these types of content under Primary Priority Content (PPC) and Priority Content (PC). Due to similarities in how some kinds of harmful content manifest, and in how they are treated in the relevant evidence base, we have grouped the 12 kinds of content into eight broader categories: pornographic content; suicide and self-harm content; eating disorder content; abuse and hate content; bullying content; violent content; dangerous stunts and challenges content; and harmful substances content. Non-designated content (NDC) is a distinct category of content in the Act. It is defined as content that is not PPC or PC, but which presents a material risk of significant harm to an appreciable number of children in the United Kingdom".

Nexus Response

The Causes and Impacts of Online Harm to Children

On Ofcom's assessment of the causes and impacts of online harms, we would like to see further detail on the kind of harmful content, as defined in the Act under Section 7, Table 7.1 for Pornographic Content, as shown in Section 8, Table 8.1, Section 1.

We agree with Ofcom's analysis of risk factors and content harmful to children, in particular:

For Pornographic Content:

- We agree that girls are more likely to experience harmful sexual behaviours, receive unwanted images, and be the subject of pornographic content.
- We agree that boys are more likely to be targeted and influenced by pornographic content
- We agree that young LGBTQIA+ people use pornographic content to learn about LGBTQIA+ sexual relationships, oftentimes due to a lack of inclusive Relationships and Sexuality Education.
- We welcome the recognition that Generative AI and deepfake technology is playing an increased role in exposing children to harmful content.
- We also welcome Ofcom's recognition of the role that direct messaging, tagging, commenting and commercial ad functionalities play in exposing children to harmful content.

For Abuse and Hate Content, and Violent Content:

- We agree that girls are more likely to experience misogyny and sexism due to their gender online
- We agree that children from diverse racial background are more likely to experience racism online
- We agree that LGBTQIA+ children are more likely to experience homophobia and transphobia online
- Protected groups are more likely to experience abuse and hate content, and violent content through social media, video sharing, livestreaming, and gaming

We agree that the use of anonymous profiles, private vs open profiles, direct messaging and tagging can increase the risk of children being exposed to harmful content.

It is important that, whilst identifying content that presents a risk of harm to children, services do not allow content that does not present as Primary Priority (PPC) or Priority (PC) to be included in a service's assessment of risk of harm to children.

We would like to highlight the growing use of "Sextortion", which involves "the threat of sharing images or videos – often 'nudes' or sexually explicit content – to extort money or force someone to do something against their will". The Revenge Porn Helpline reported that sextortion cases increased by 54% in 2023 compared to 2022, with 825 support requests coming from children aged 13-18, and 170 requests from children under the age of 13. The PSNI reported that sextortion cases had jumped from 5-10 reports per month in 2019 to 75-80 cases per month in 2023, with the majority of victims being young men between 18 and 23 years old. The National Crime Agency issued an urgent warning following a "considerable increase in global cases of financially motivated sexual extortion... a large proportion of cases have involved male victims aged between 14-18. Ninety-one per cent of victims in UK sextortion cases dealt with by the Internet Watch Foundation in 2023 were male".

Through our work with children and young people, we have also come across a concerning trend using "Live" features on TikTok, Instagram, and Facebook to target children and young people with sexual content.

We also included the following research on the risks of Generative AI to children:

From the Internet Watch Foundation Report on AI Child Sexual Abuse Imagery -

- "In total, 20,254 AI-generated images were found to have been posted to one dark web CSAM forum in a one-month period".
- "Perpetrators can legally download everything they need to generate these images, then can produce as many images as they want – offline, with no opportunity for detection. Various tools exist for improving and editing generated images until they look exactly like the perpetrator wants".

- “Most AI CSAM found is now realistic enough to be treated as ‘real’ CSAM”.
- “There is now reasonable evidence that AI CSAM has increased the potential for the re-victimisation of known child sexual abuse victims, as well as for the victimisation of famous children and children known to perpetrators”.
- “AI CSAM offers another route for perpetrators to profit from child sexual abuse”.

The National Crime Agency said in their 2023 National Strategic Assessment that “We have also begun to see hyper realistic images and videos entirely created through Artificial Intelligence. The use of AI for child sexual abuse will make it harder for us to identify real children who need protecting, and further normalise abuse. And that matters, because we assess that the viewing of these images – whether real or AI generated - materially increases the risk of offenders moving on to sexually abusing children themselves. There is also no doubt that our work is being made harder, as major technology companies develop their services, including rolling out end to end encryption, in a way that they know will make it more difficult for law enforcement to detect and investigate crime and protect children”.

The Stanford Internet Observatory conducted an investigation that identified “hundreds of known images of child sexual abuse material in an open dataset used to train popular AI text-to-image generation models”. The report found that “Models trained on this dataset, known as LAION-5B, are being used to create photorealistic AI-generated nude images, including CSAM”.

The UK Safer Internet Centre reported that “schoolchildren in the UK are now using AI to generate indecent images of other children, with experts warning urgent action is needed to help children understand the risks of making this sort of imagery…. Children may be making this imagery out of curiosity, sexual exploration, or for a range of other reasons, but images can quickly get out of hand and children risk "losing control" of the material, which can then circulate on the open web". The Centre also says that "this imagery can have many harmful effects on children – and warns it could also be used to abuse or blackmail children".

Draft Guidance on Content Harmful to Children

Nexus agrees with the proposed approach to the draft Guidance on Content Harmful to Children. Providing a non-exhaustive, illustrative list of example content that may or may not constitute PPC, PC, or NDC balances clarity for services to identify potentially harmful content with applicability, thereby not limiting services to only the examples provided. We welcome Ofcom's guidance on how content can be highly subjective and context specific, meaning that different kinds of harms can vary in nature due to the presentation of the content and the specific nature of the user and poster. We also welcome Ofcom's efforts to differentiate between content harmful to children and recovery content, which can be beneficial for children and other users who are on or beginning a recovery journey. Ofcom provides guidance for services to determine the nature of the content, as discussed above.

For specific content sections:

- We agree that, for Abuse and Hate Content, that hate and abuse can overlap with Violent Content, particularly in the case of abuse, hate, and violence towards women and girls.
- We also agree that hate and abuse can be present regardless of whether the individual or group targeted holds the listed characteristic, or they are perceived to hold said characteristic. This is important to recognise, as stereotypes, typecasting, and false and misinformation can generate hate and abuse towards individuals and groups with listed characteristics.
- We welcome Ofcom's recognition of gender-based violence and sexual violence in the Violent Content section, particularly including content which:

- Justifies and/or defends the use of sexual violence
- Commends domestic abuse as a means to ‘control’ women
- Argues that victims and survivors of sexual assault must bear some responsibility

We agree with the proposal to include codewords, hashtags, substitute terms/phrases, sounds, pornographic GIFs, sexualised emojis, and comments as elements for services to consider as content that poses a risk of harm to children. The Internet Watch Foundation has a curated Keyword List that compiles words, phrase, and codes for concealing child sexual abuse material online.

We have a point of clarification for 8.2 Guidance on Pornographic Content- in 8.2.7, Ofcom outlines the elements that will make it more or less likely for the content to be deemed as having the principal or sole purpose of sexual arousal, which includes “Very strong references to sexual behaviour: Use of language associated with sexual activity and pornography e.g. ‘milf’, ‘horny’”. Then, in point 8.2.8, Ofcom states that “However, if content depicts an individual using pornographic language but they are fully clothed and not carrying out or simulating sexual activity this would likely not be judged to be pornographic”. We would appreciate some clarification around when the use of language strongly associated with sexual activity and pornography is considered to be pornographic content. We have found from our engagement with young people that they don’t often use explicit, sexualised language and are more likely to use acronyms, emojis, and other code words to convey sexualised content. We would therefore also like clarification on the definition and context of non-sexualised GIFs and emojis, and the guidance for services to interpret these functions in the context of the post.

Volume 4: Assessing the risks of Harm to Children Online

In this volume, Ofcom explain their proposals about the governance measures service providers should put in place to manage risk to children and how service providers should go about assessing the risk of harm to children encountering harmful content online.

Nexus Response

We agree with the proposed governance measures. There is a balance of accountability between governance, senior leadership accountability, internal monitoring, and staff policy implementation to create a holistic approach to governance and accountability. As we stated in our submission to Question 3 of the Ofcom Consultation on 'Protecting People from Illegal Harms Online', designating and training senior members of staff to make decisions on online safety as well as track evidence of risk in their services is vital to adapting to new challenges and maintaining accountability. We would like to reiterate, however, that assessing risk is often complex and nuanced, and needs supported by other forms of specific training on CSE, CSA, Safeguarding, Child Protection, etc.

We believe that the proposals in relation to the Children's Risk Profiles are comprehensive and informative. The Profiles provide a succinct guide to assist services with identifying high risk factors in different aspects of their content. It is vital that Ofcom creates guidance and assessments that remove any guesswork on behalf of services and directly highlight the harms that children are at risk of coming into contact with and therefore ensures that services completing their Risk Assessments are not self-eliminating their services. Ofcom's Risk Profiles will describe how the risk arises and what kind of content is relevant to perpetuating said risks by directly recognising the links between service capability and child user experiences.

We agree that implementing the same process for the Children’s Safety Codes and the Illegal Content Codes would ensure consistency across service provision, accountability, and innovation. We also appreciate the emphasis on the detrimental effects of poor governance and accountability on children and vulnerable people, especially if there is a disjointed approach across different codes. The proposed codes are in line with a user-centred approach and has been informed by children and vulnerable people’s safety.

Volume 5: What should Services do to mitigate the risks of Online Harms to Children?

Volume 5 outlines draft measures Ofcom propose providers of services likely to be accessed by children could take to comply with their child safety duties in the Online Safety Act. These are set out in the draft Children's Safety Codes in Annexes 7 and 8, which will be finalised following consultation, including age assurance measures, content moderation, search moderation, user reporting and complaints, terms of service, recommender systems, user support, impact assessments, and statutory test.

Nexus Response

We agree with the measures proposed in the Children's Safety Codes, with some recommendations:

We would recommend that, under measure PCU E3, in *Signposting child users to support of the Protection of Children Code of Practice for user-to-user services*, Ofcom include the following in **bold red font**:

"Services likely to be accessed by children where there is a medium or high risk of bullying content, eating disorder content, self-harm content or suicide content, **sexual abuse content, domestic abuse content, content containing or pertaining to violence against women and girls, and content containing or pertaining to racism, ableism, homophobia, transphobia**".

As evidenced by the following research:

- Ofcom's Children's Media Lives 2022 Report, "around a third of the participants were engaging with content about racism" and a research study conducted in January 2024 found that Black children and teenagers who experienced racism online were at risk of developing post-traumatic stress disorder.
- Stonewall's 2017 School Report found that 40% of LGBTQ+ young people have been the target of homophobic, biphobic and transphobic abuse online.
- Cornell University research found that social media and online platforms were being used to amplify microaggressions, spread misinformation, and discriminate against people with disabilities.
- Internet Matters conducted a report on Online Misogyny, finding that "half (50%) of boys aged 15-16 and over half (55%) of girls aged 15-16 believe that the online world has made misogyny worse".

Age Assurance Measures

We recognise the need for a levelled approach to measures for different services according to risk, size of service, functionalities, and type of service. This will ensure that services that are assessed to be medium to high level of risk, are of a larger service user base, and/or present multi-risks are held to a higher standard of measures and duties. However, we want to emphasise the need for employing the expertise to continually scope for software that might be able to bypass the age assurance technology as this landscape would move quickly. It is vital that the age assurance technology is accurate at determining the age of a user. This includes constant and varied testing of the technology. The guidance deals fairly with the concerns of bias, wrongful exclusion, and discrimination. Service users should ensure that they are not preventing adults from accessing legal content, and as such this criterion emphasises the need for age assurance technologies to be tested with diverse backgrounds, needs, and datasets.

Content Moderation

We agree with the proposals on content moderation for user-to-user services. Section 16 is clear on the serious risks of ineffective content moderation, which underpins the explanations of each measure. There is a balance between what services should be doing through the service they offer and what internal work they should do to train, resource, and support their service moderators. Ofcom's recommendations include cost-effective, proportionate measures for all services, with extra requirements for large and multi-risk services whereby there is a greater need for protecting service users. We also welcome Ofcom's commitment to an additional consultation later this year on automated content moderation and detection tools, as we see a growing trend in online technology turning to automated features, AI content and recommendation functions, and automated customer support.

Search Moderation

We agree with the proposals in this Section. Downranking, blurring, and filtering PCC and PC content when the user is believed to be a child will protect the user from harmful content and any recommender system prompts. As in our answer to questions on Age Assurance measures, we would like to emphasise the need for services to employ rigorous testing and scoping for any technologies that can enable bypassing or circumventing search moderation and age assurance technologies.

User Reporting and Complaints

We agree with the proposed measures for user reporting and complaints. Particularly, we agree that services should create accessible, easy to understand, and transparent complaint and reporting systems that will appeal to children and vulnerable services users and thereby increase the likelihood of harmful content and user profiles being reported. From multiple discussions with young people, they rarely report or use reporting systems. When in discussions with classes of 11–12-year-olds who disclosed regularly receiving unwanted sexual images through DMs on a social media platform, they stated that they block the person and don't report as "what's the point" and because it happens nearly daily, they felt blocking was easier and more instant.

We have included a section of our submission to the Ofcom ‘Illegal Harms’ Consultation- “Nexus would like to highlight the importance of support for children using a service when they identify content that is illegal and harmful. In particular, we would recommend that Ofcom include strict guidance for services to ensure that their complaints procedure is robust, simplified, and accessible; for example, once a complaint has been made by a child user, will the content and/or profile that has been reported be suspended pending investigation? Alongside this, will service platforms provide support information after a complaint has been made? And are there measures for parents, guardians, carers, or a nominated caretaker to make a complaint on behalf of the child?

These are only some examples of measures to protect children and young people online that Ofcom can recommend to services as part of their safeguarding measures”. It must be clear and easy to understand but more importantly, as simplified a process as possible as young people tell is there's no point in reporting as it's often "overruled" or it takes too long. There is evidence that children are unfamiliar or unaware of the procedures with reporting and whether any identifying information will be included in the report. Children are already facing mounting peer pressure online - Ofcom’s Children’s Media Literacy 2024 Report found that “87% of users of these apps of this age agree that there is pressure to be popular on social media and messaging sites/apps, at least some of the time”- so it is important that any reporting features are clearly laid out and informative for users as to inform their decision to report a post or user.

Terms of Service

We agree with the proposed Terms of Service and Publicly Available Statements measures. In order to be accessible and informative, Terms of Service/Publicly Available Statements need to comply with the Online Safety Act, contain clear language, and keep users informed of harmful content and how to get support from the service. We believe that language, presentation, and length of the document are key considerations for engaging children, young people, and vulnerable users in the Terms of Service. By creating a Terms of Service and/or Publicly Available Statement that is engaging and relates to the interests of young people- such as highlighting the importance of mental health, how to spot harmful content, and where to go for help and how the service will respond to your report- will increase the likelihood of children and young people engaging with the Terms of Service/ Publicly Available Statement. One suggestion that we have found accessible to engage young people is through audio and visual mediums as opposed to text. By engaging our different senses, we can capture the attention and retention of children and young people, as well as educate parents, carers, and teachers through an accessible format.

Recommender Systems

We agree with the proposed recommender system measures. As discussed in the draft guidance, recommender systems can create a constant stream of harmful content for child users, making it harder for child users to avoid triggering content. Content that might, on the surface, not appear to be harmful can quickly be used to inform recommender algorithms and push harmful content onto children's feeds, profiles, and 'for you' pages. Machine learning will identify content that is being engaged with and will identify users through hashtags, location, music, etc. and will recommend further content. Children are at risk of coming across content that they may not wish to see, but because they have engaged with it, they will continue to be recommended said content. The following research illustrates the risks of recommender systems:

- Investigation by the Institute for Strategic Dialogue found that YouTube's recommender system routinely pushes extremely misogynistic hateful material into boys' feeds.

- Amnesty International found that "Between 3 and 20 minutes into our manual research, more than half of the videos in the 'For You' feed were related to mental health struggles with multiple recommended videos in a single hour romanticizing, normalizing or encouraging suicide".

- A report by The Centre for Countering Digital Hate titled 'The Incelosphere' found that "YouTube channels are hosting incel channels with over 136,000 subscribers and Google search surfaces incelosphere sites on searches related to key incel concerns, like improving physical appearance". The term 'incel' is shorthand for 'involuntary celibate' which has come to represent, as Founder of the Everyday Sexism Project Laura Bates said, "male-only spaces that blame their members' problems on women, promoting a hateful and violent ideology linked to the murder or injury of 100 people in last ten years, mostly women".

- Alongside incels, there is a growing body of so-called 'femcels', who believe that "the toxic and unrealistic body standards that are set upon women by society, they are unable to find a sexual partner or form a romantic relationship". According to research in the Archives of Sexual Behaviour, femcels were "more interested in their own frustrations than men's frustrations" such as improving their attractiveness and desirability to achieve features including, as Psychology Today reports, a "symmetrical face," "short philtrum," "full lips," "small noses," "positive eye tilt," "smaller foreheads," "neotenous features," and a "smaller jaw/chin". Glamour Magazine's piece on Femcel Culture also raised concerns of femcel communities engaging in transphobic language, body shaming, and fatphobia.

User Support
We agree with these proposals, and we see the importance of these proposals being rolled out to all users. In the consultation document, it is noted that Measure US2 (Option to block and mute other accounts) is included as Measure 9A in the Illegal Harms Codes, and Measure US3 (Option to disable comments) is included as Measure 9B in the Illegal Harms Codes. However, we would recommend that Measures US1, US4, US5, and US6 are incorporated for all service users as well to protect people from harmful content.

Search Features, Functionalities, and User Support
We agree with the proposals in this Section. We would like to recommend, however, that Measure SD2 is amended to include the following in bold red text "crisis prevention information in response to known PCC and **PC-related search requests** regarding suicide, self-harm, eating disorders, **sexual abuse content, domestic abuse content, content containing or pertaining to violence against women and girls, and content containing or pertaining to racism, ableism, homophobia, transphobia**". Our research base for this can be found in our answer to the proposed draft Children's Safety Codes.

From our work with children and young people through our Early Intervention and Prevention workshops, we have found the following: When looking at our Body Positivity module, the young men and boys we have worked with have spoken about the pressures of "looksmaxxing", a rapidly growing trend that targets mostly boys and young men to critique their physical appearance, score themselves on a scale of 'manliness', and aim to increase their 'scores' to achieve the 'peak male appearance'. Looksmaxxing preys on the insecurities of young men and boys to physically alter themselves using different exercises, filters, and influencer routines and products in order to appear more attractive. Young men and boys are searching TikTok and Google for tips, products, and inspiration for achieving this look, which is then fuelled by algorithmic recommender systems to continue to feed this content, with the risk of young men and boys venturing into incel spaces without recognising it; Mike Nicholson, a former teacher who runs a workshop programme called 'Progressive Masculinity' has said that "the world that these young men and boys are inhabiting is one that is trying to increase their anxieties and potentially lead them down this path that, if you're not careful, can lead to 'incel' ideologies".

In the same module, young women and girls are reporting the pressure to use filters to alter their appearances, using social media to search for content that promotes appearance-alerting products and procedures. According to a 2021 survey of 200 teens ages 13 to 21 from ParentsTogether, young people who use beauty filters weekly are more likely to want to have cosmetic surgery and to alter their skin colour. With a recommender search system, young women and girls are at risk of being recommended the kinds of products that claim to alter appearances to achieve a desired attractiveness, such as cosmetic procedures, dangerous dieting information, and extreme exercise. The Campaign Director for ParentsTogether, Amanda Kloer, told Teen Vogue that "there's also a big problem with the kind of content that these algorithms amplify. For example, if you're a young girl and you start an Instagram account, you get so much diet and exercise content, even if that's not something you indicate that you're interested in".

Conclusion

We welcome the comprehensive, equitable, and supportive work that Ofcom have conducted with their draft Publications for Protecting Children from Harms Online. As we have mentioned throughout our submission, proposals are rigorous and intentionally wide-ranging to capture all aspects of service provision, business practises, and child user activity.

Overall, the proposals are detailed, extensive, and accessible for service providers. It is clear that risk of harm for children needs to account for and recognise each kind of harmful content, the likelihood of a child interacting with the harmful content on the service, the effectiveness of existing safety measures, the impact the content on children- both directly and indirectly- and the severity and reach of the content. The 4-step model for the Risk Assessment Process is clear, concise, and informative. Each step provides the background rationale contained in the Online Safety Act, the explanation of each supplementary guidance document, and the expectations for actioning each step, which continues to build consecutively as you move through each step. There is great emphasis placed on not just assessing harms but also assessing how services are used, the risk of repetitive and cumulative harms, and the duty to recognise and respond to changes, triggers, and new developments.

It is important that the implementation of the Online Safety Act captures both legal and illegal content as a measure to protecting children online. As discussed throughout our consultation response, children access harmful content on a variety of social media apps, online websites, chatrooms, video games, etc. which are not always illegal by design. In order to effectively protect child users, we agree that there needs to be two separate Codes that work together to protect children.

As an organisation that facilitates training and workshops to children and young people, we are concerned about the growing use of "sextortion" as a tactic for sexually exploiting young people. We would like to see this reflected in Ofcom's risk assessments guidance, as well as clarification on the Guidance for Pornographic Content, specifically the use of language, emojis, GIFs, and alternative forms of sexualised language that is not text-based. We would also like to see the Children's Safety Codes and the Measures for Search features expanded to include content that contains sexual abuse, domestic abuse, violence against women and girls, racism, ableism, homophobia, and transphobia.

We know from our work with a wide range of businesses, organisations, and other key stakeholders that assessing risk is complex and nuanced, and so we would recommend Ofcom highlight to services the need for additional training in Child Sexual Exploitation, Child Protection and Safeguarding, and Child Sexual Abuse. Ensuring that staff and technologies are trained, and staying up to date with any new advancements is imperative to protecting children online.

Finally, we want to reiterate our recommendations for creating accessible, clear, and alternative ways for terms of reference and complaints procedures to be created to reach more children and young people who might need support online as well as being entirely informed before consenting to use a service.

Further Information

For more information please contact the Nexus Communications Team using the details below:

Nexus
59 Malone Road
Belfast
BT9 6SA
028 9032 6803
nexusni.org
communications@nexusni.org

BACP Accredited
Service
No. 101852
Charity Commission Reg
No. NIC102558