



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	Commissioner Designate for Victims of Crime Northern Ireland

The Commissioner Designate for Victims of Crime in Northern Ireland was established to:

- Provide a voice for all victims of crime;
- Identify, promote, encourage and issue guidance on good practice;
- Review the adequacy and effectiveness of law and practice;
- Review the operation and delivery of Charter entitlements;
- Direct complaints and monitor outcomes;
- Advise and make recommendations; and
- Undertake and commission research.

We want to see a society where victims of all crime feel valued and have rights to protection, participation, support and redress.

As an office still in relative infancy, our capacity limits our ability to conduct thorough research and gather sufficient evidence to provide a comprehensive response to Ofcom on this issue.

We encourage Ofcom to pay particular attention to submissions made by the Northern Ireland Commissioner for Children and Young People (NICCY), the NSPCC and the Victims Commissioner in England and Wales.

We will continue discussions with the government and Ofcom as appropriate to ensure that the voices of victims of crime in Northern Ireland are heard throughout the consultation process. This response is based on our experience on engaging with and supporting victims of crime.

We believe that technology and the online space have the potential to provide great benefits to all, including children.

However, there is also a high risk that children will access harmful content and may even become victims of crime. We are also aware that some children are at greater risk than others and that it is important to remember that risk factors often overlap.

We know from our engagement with victims of crime that there is a world of criminals waiting to take advantage of people online through scams, fraud, technology assisted abuse, sexploitation and a range of other crimes that can impact children.

We also know that accessing harmful content online has a real and detrimental impact on people in the real world. Working closely with victims of domestic and sexual violence and hate crime it has been possible, supported by a range of academic research, to draw a direct line between harmful online content and the spread of misogyny, racism and other forms of hatred. The Victims Commissioner in England and Wales report, *'The Impact of Online Abuse: Hearing the Victims' Voice'*¹, demonstrates how online abuse and harassment can cause significant emotional harm to victims including feelings of anxiety, depression and social withdrawal. This report also found that only 14% of victims surveyed agreed that the company were helpful in assisting them when making a complaint.

Victims of sexual and domestic abuse have often told us how important they believe effective relationship and sexuality education (RSE) is in terms of educating individuals to identify negative behaviours and remove themselves from unhealthy relationships. A critical, and relatively new, component of good RSE involves improved digital literacy. Artificial Intelligence has a range of potential benefits, however, in its current state it poses a great

¹ [The Impact of Online Abuse: Hearing the Victims' Voice - Victims Commissioner](#)

and unquantified risk to young people. GenAI, particularly its ability to create deep fakes and the image based abuse that can follow, is of particular concern to this office.

The interconnectedness of online and offline experiences means that the impact of online harm can often extend beyond the digital sphere, reinforcing a cycle of victimisation specifically for children who are being bullied and harassed at school. It is essential that all service providers take a proactive approach which enables children to enjoy the benefits of the digital world where appropriate safeguards are in place.

Through the rest of this document we will comment on specific issues raised in the consultation questionnaire.

Volume 2: Children's Access Assessments

We agree that it is vitally important for all online service providers to carry out access assessments and agree that they should only conclude children are not able to access it where they use a highly effective age assurance.

We believe that the presumption must be that children are accessing or able to access the service and that only demonstrably effective age assurance should be considered as effective.

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

We agree that service providers should err on the side of caution and would encourage guidance to direct all service providers to operate on the assumption that children will access their service unless they can demonstrably prove children will not access it and act accordingly.

The requirement for providers to publish a summary of their risk assessment in their Terms of Service is also welcomed. Such information must be accessible and easily understood and we if it is to achieve the desired aim. We would particularly welcome therefore a requirement for companies to ensure that the summary of risk is presented in a way that ensures clarity of understanding to the lay reader and is easily accessible, this not only helps promote transparency but also assists decision making by children and parents.

It should also be reflected in the guidance that children will often attempt to access material that is specifically **not** for them. The criteria laying out what might be appealing to children talks about content that is entertaining or educational, but this should be broadened out to also reflect the fact that children are naturally curious and will often try to access content they do not know about, whether it is age appropriate or not. This is reflected in the high percentage of young children who have been exposed to harmful content including pornography and should be an important consideration for service providers when making these decisions.

Volume 3: The causes and impacts of online harm to children

We welcome the fact that Ofcom has gone to considerable effort to speak to a large number of children and parents in relation to the assessment of the causes and impacts of online harm.

We are aware that NICCY have worked with a panel of children and young people and we would strongly support their voices being heard as part of this process.

We agree with the analysis that links viewing of pornography, especially violent pornography, at a young age with an unhealthy attitude towards relationships at a later stage in life and the normalisation of sexual aggression and harmful sexual behaviours towards girls.

We believe, from engaging with victims of domestic and sexual abuse, that it is also important to consider the next stage and how this unhealthy attitude towards sexuality and relationships can be a factor in individuals committing domestic or sexual crimes later in life.

This is an important issue to consider when looking at long term risks of harm to children.

In a previous consultation response, the Commissioner for Victims of Crime in England and Wales highlighted the need to *not work on the assumption that the online space is neutral or good and to not work on the assumption that service providers are good faith actors*. We welcome the acknowledgement in this document that the business models of certain service providers depend upon directing individuals towards harmful content to drive up engagement and encourage advertisers.

We welcome the prevalence given to content recommender systems as a risk factor across the different content harmful to children and the acknowledgement that characteristics of children including sex, disability, race etc. can further increase the child's risk of engaging with harmful content.

However, Ofcom should be bolder in working towards stopping service providers from using algorithms and recommender systems to drive children towards potentially harmful content in order to drive up their own profit.

We believe the contextual information is really important and this should be considered by all service providers. Service providers should be aware of the intersectional risk factors that can increase the risk of harm to children. We support the Victims Commissioner for England and Wales who in a response to another recent consultation said that it is important to consider the cross-cutting impacts harmful content can have on children and to carefully consider the real world impacts online content can have.

We also agree with the previous response from the Victims Commissioner in England and Wales when they identified the issue of specifying harms can create a perception that the content can be siloed. This is particularly problematic given evidence that shows that people who access one type of harmful content are often exposed to other harmful content.

Given Northern Ireland's history, we believe harmful content related to sectarianism or the glorifying of paramilitary gangs could be included as a separate and distinct category.

Volume 4: How should services assess the risk of online harm?

It is vital that services have appropriate assurance, oversight, awareness-building and internal reporting processes in place to support the management of risks identified in children's risk assessments. We welcome the awareness that responsibility belongs to everyone in each organisation at all levels.

We encourage Ofcom to consider recommending that providers proactively engage and collaborate where appropriate with child safety organisations to assist them in their governance in this area. Such partnerships can help develop innovative solutions, build expertise and support a safer online environment.

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

We believe the emphasis should be on service providers to proactively prevent harmful content being available to children rather than on retrospective measures such as takedown and blocking which require actions by the user. The emphasis must be on service providers to make sure their algorithms and recommender systems are safer.

We agree with the NSPCC that it is concerning that there are no measures requiring services to use some form of automated content moderation, particularly for large or multi-risk services.

The Children's Safety Codes Framework must be weighted so that the rights of children to avoid being harmed by harmful content outweighs other rights such as freedom of speech and other considerations such as direct and indirect costs.

We agree that there is logic in allowing service providers to use systems and processes to manage both content harmful to children and illegal content, however there must be an assurance that there is no degradation of protections by using one system or process and that if service providers should have an obligation to provide clear evidence that using the same system or process for both provides adequate protection in both instances.

We would encourage protections to be applicable to all service users regardless of size, especially as new service providers come into the market. Children and young people are the first adapters of new online service providers generally, therefore even if an organisation is small it should have the same requirements to protect children from harmful content, regardless of cost.

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

We strongly echo arguments previously made by the Victims Commissioner in England and Wales and others that the emphasis must be on service providers to proactively moderate harmful content. The reliance should not be on people to act against harmful content after it has been published and viewed by individuals. We believe that there should also be more encouragement for service providers to take a proactive approach that uses a combination of human moderators, AI or other automated tools to identify content that may be harmful and moderate it before it is posted and could possibly be accessed by children,

We support the need for complaints procedures to be clear, straightforward and accessible. Where harmful content has been flagged by a user, providers must be required to take immediate steps to remove it. Feedback from victims has unfortunately highlighted difficulties in contacting social media platforms in such circumstances and a slowness to act to address issues.

As an office, we are particularly concerned with the potential risks of GenAI. We would encourage Ofcom to continue to monitor this and work closely with the appropriate stakeholders to adapt these protections for children.

One section in the User Reporting and Complaints Section mentions the ability of children to decline invitations to join a group chat, however we believe that no-one should be able to invite a child into a group chat without serious protections in place.

We agree that it is right to apply Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints on the basis that responsibility should be shared by all service providers regardless of size.

We strongly echo concerns raised by the Victims Commissioner in England and Wales about the potential negative impact that recommender systems can have.

We also agree that it is vital that these recommender systems and the business models that rely on driving people to harmful content should not be considered as good faith actors and the online space should not be considered a neutral space.

We believe that where a service provider cannot guarantee that a user is an adult, the default recommender system should have the protections needed for children.

We agree with the NSPCC that there is a higher risk of harmful content being shared in private messaging and *that "Ofcom must pre-empt the risk of harm increasingly migrating from public to private spaces and introduce robust measures for private messaging services now."*

We do agree with the proposal that non-designated content (NDC) namely depressive content and body image content be included in RS2 and RS3. We believe it is important that there is an awareness that NDC can cause harm to children and would encourage Ofcom to widen the scope beyond just the two mentioned here. We would encourage Ofcom to work closely with children's organisations to investigate what other NDC could be included under this consideration.

However we would agree with concerns raised by some that it is also vitally important that service providers who provide support are not caught up in this inadvertently. For example a charity that supports young people with mental health issues should not be flagged as producing potentially harmful content because they talk about depression and anxiety.

We welcome Ofcom's work in this area and encourage them to continue to be guided by the expertise of those working with children and young people and other relevant experts in this field it is vitally important that children are protected from accessing harmful content. This responsibility must fall on the shoulder of service providers who have a duty to provide their services in a safe way.