NSPCC

Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

21 March 2023

NSPCC's response to the 'Call for evidence: Second phase of online safety regulation.'

The NSPCC welcomes the opportunity to respond to this call for evidence on Ofcom's approach and plans for protecting children from legal but harmful content online. We were encouraged to hear Ofcom's Chief Executive, at her recent appearance at the DCMS parliamentary Select Committee, speak of the need for partnerships as Ofcom carries out its statutory duties and to mention the NSPCC in this context. In the spirit of supporting Ofcom's work to ensure the Online Safety Bill delivers for children, we would be happy to meet with Ofcom to discuss any of the points raised in this consultation response in more detail.

The NSPCC has made keeping children safe online a focus of our strategy to stop child abuse across the UK. In response to the increasing amount and complexity of harms being experienced by children and young people, we have ramped up our efforts around online safety and made concrete progress on improving legislation, practice and awareness through our research and policy work, campaigning, e-learning and workshops with parents and carers. We continue to learn about the opportunities and challenges presented to children by a rapidly developing technology landscape through our services and helplines.

The NSPCC supports children by providing access to Childline for free support and advice 24 hours a day, 7 days a week and through developing tools like Report Remove which helps children remove sexual images or videos of themselves from the internet. We are also seen as a 'Trusted Flagger' by certain online service providers which allows us to directly report harmful content that should be removed with these reports being seen as priority content by the service providers.

The NSPCC, alongside 5Rights, is supporting and working alongside a group of bereaved parents who have direct experience of the impact of online harms on children and young people. This includes Ruth Moss (mother of Sophie Parkinson), Ian Russell (father of Molly Russell), Andy and Judy Thomas (parents of Frankie Thomas), Lorin La Fave (mother of Breck Bednar) and Amanda and Stuart Stephens (parents of Olly Stephens). Their experiences have informed some of the points we make in this consultation response. We know they are talking directly with Ofcom and sharing their feedback as part of this exercise. The NSPCC will continue to support and work with them to amplify their important messages about preventing avoidable harm to children online.

Over the next three years, we will also be focussed on amplifying the voices and experiences of children and young people online including increasing our capacity for participation and advocacy with them and ensuring they can participate in online safety debates and decision-making. We will be learning more about children's experiences online - through targeted engagement, bespoke research, and access to data streams - so that we can shine a spotlight on new and emerging harms and work to design solutions to the problems they face.

Our answers to the consultation questions aim to provide a principled response and share relevant supporting evidence. We focus on identifying harms rather than specific tools to mitigate harm. We are conscious that each platform is different and will have bespoke risks, and "one size" will not fit all. We have therefore not shared an exhaustive list of the harms which we are aware of or their prevalence on particular platforms. We would however be happy to discuss how best to share some of that information with Ofcom if helpful.

Three overarching points are woven into our responses:

1. **The importance of listening to children's voices**: Children and young people are the experts on their own lives and have unique, important insight and experience of the realities of being online that are vital for decision makers to seek out, hear and act on. Ofcom and online services must listen to children and those that represent children as they make regulatory decisions and design choices which impact children. This should include having permanent lines of communication with the children's sector to best understand the landscape of current and future harms to children online.

   As Ofcom knows, the NSPCC is calling for user advocacy arrangements for children to be introduced in the online safety regime. We believe this is the best way to ensure that children's voices and experiences are taken into account in regulatory decisions and platform design. Further information on our policy ask can be found here.

2. **Greater data transparency:** Data scarcity prevents all parties from having a full understanding of the landscape of online harms. Without an understanding of the risks to children collected in real time from services on the ground, Ofcom and online services will struggle to effectively risk assess their platforms. Additionally, civil society, researchers and academics need access to the data and insights of online platforms to gain an understanding of emerging issues, trends and patterns on platforms. This will enable us to better support children and young people – including through the design of new services. Ofcom has a vital role to play in fixing the gaps in information in this market.

3. **Cross-UK approach to regulation:** Whilst the Online Safety Bill is a UK Bill and there are commonalities between the four nations of the UK, there are also important differences in the online safety landscape and we urge Ofcom to continue to engage with stakeholders across the UK and work with platforms to consider how different users in different nations may have different experiences and needs (including around language).

If you have any questions regarding any part of the response, please contact us via richard.collard@nspcc.org.uk.

**Note – Please note that we have now added a confidential annex to this response in order to share the insights of a member of NSPCC's Young People's Board for Change. [4 May 2023]*

Yours sincerely,

Associate Head, Policy and Public Affairs

Child Safety Online
NSPCC

Call for evidence response form

Please complete this form in full and return to os-cfe@ofcom.org.uk

Title
Second phase of online safety regulation: Protection of children

Full name
✂

Contact phone number
✂

Representing (select as appropriate)
Organisation

Organisation name
NSPCC

Email address
✂

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? (select as appropriate)
Nothing

Your response: Please indicate how much of your response you want to keep confidential (select as appropriate)
Part of the response (you will need to indicate below which question responses are confidential)

For confidential responses, can Ofcom publish a reference to the contents of your response? (select as appropriate)

Yes

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.

Is this a confidential response?

No

The NSPCC is the UK's leading child protection charity with over 130 years in experience of safeguarding children from harms. We have led the campaign for online regulation and were a driving force in the introduction of the Online Safety Bill. We are committed to ensuring that children are safer online and intend to contribute to creating a regulatory regime which incentivises online service providers to embed safety by design when creating new products.

We are committed to using knowledge and expertise to raise children's voices in the debate, and support the development of a strong, child-centric, regulatory framework which reduces harm for children online.

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

Is this a confidential response? (Select as appropriate)
No

What becomes popular online is hard to predict and will frequently change. We welcome the research Ofcom has commissioned to help understand children's media lives and would expect this is repeated on a regular basis (Revealing Reality (2022) *Children's Media Lives: A report for Ofcom).*

To help respond to the dynamic, evolving nature of child users' engagements with services, we believe Ofcom needs to have access to real time data on children's use and exposure to risk through platform information, participation with children and young people, helplines and other data sources.

In line with the safety-by-design ethos of the online safety legislation, the default assumption should be that children may attempt to access any service. The assumption that children are not using a particular service should only be made by providers if there is evidence that 100% of the users are adults. The regulator should not create a situation whereby a platform can claim exemption from their child safety duties because their platform was not intended to be access by children (i.e., OnlyFans).[2]

Question 3: What information do services have about the age of users on different platforms (including children)?

Is this a confidential response? (select as appropriate)

No

Services do have information about the age of their user base, and they already use it to make some decisions about the service they provide. Targeted adverts depending on the child's age range, are a clear indication that platforms are collecting and using data on children's activity online. Companies should adhere to the principles of the ICO's *Age Appropriate Design Code* (Children's Code) to ensure that the default is minimal data collection without compromising on children's access to online services.

We would expect platforms to be sharing information on the age of their user base in their public risk assessment summaries. Understanding the age of users is one of the key components for providing an age appropriate service and mitigating harms to children and platforms must be transparent about this.

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

No

Children have a right to be online. It is a place where they learn, play and communicate. We are conscious that some platforms may look to alter their terms of service and ban children as a way of avoiding having to comply with the child safety duties. As Ofcom designs its regulatory framework, it would be helpful to avoid inadvertently incentivising platforms to block children from services which benefit them.

In circumstances where a service or content on a service is not age appropriate, we would expect platforms to use sophisticated and privacy preserving age assurance technologies to stop the user being exposed. We expand on this in question 5.

For further detail on this please see NSPCC's response to Q18 of the "First phase of online safety regulation" (p. 13 – 14).

Question 5:What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Is this a confidential response? (select as appropriate)

No

Age assurance (AA) and age verification (AV) are evolving and improving and will be key tools for companies to ensure online service providers are complying with their child safety duties, and to protect children online.

Minimum standards for AA and AV are important to ensure that these tools are fit for purpose, they deliver the intended outcomes and comply with regulation. If there are not clear, public set standards, we are concerned that AA and AV could be used as an, in effect, a loophole by companies where they implement inadequate tools – allowing them to indicate publicly that they meet regulatory requirements, without investing in the technology required to operate these systems effectively.

The regulator should also set clear thresholds for measuring the efficacy for AA and AV tools, which are proportionate to the risk of harm on a particular platform.

We know that it is possible for children to access services that are age verified if an older person provides them with access to the platform. It is important that age assurance is used in tandem with age verification to ensure that children are not exposed to age-inappropriate content by circumventing the system.

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Is this a confidential response? (select as appropriate)

No

Childline insights
NSPCC service data contains evidence of the presence of harmful content on online services. However, to preserve the privacy of people who use the services, we are careful in how we share their data.

Our publicly available NSPCC Learning Briefing: *Children's experiences of legal but harmful content online* uses insights from Childline and our NSPCC Helpline contacts. It highlights the experiences of children and young people who have viewed legal but harmful content online. Key findings include:

- Some children told Childline that they have actively searched for legal but harmful content, but most children typically "stumbled" across harmful content while on their favourite platforms.

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

- Some children told us they found themselves drawn into searching for additional and more extreme content.
- Some felt particular forms of legal but harmful content helped them to deal with difficult issues they were facing, e.g., pro-eating disorder content
- Some children and adults were confused about why certain harmful content was permitted online.
- Some adults contacting the NSPCC helpline were unclear on the role of social media companies and believed more could be done to keep their channels safe for children.

Tamsin (name has been changed) was unwittingly exposed to pro-anorexia content. Now aged 20, she was a teenager when her mental health began to deteriorate. She developed an eating disorder and was eventually admitted to an in-patient unit for eight months.

> *"My eating disorder happened so quickly. Something in my brain just suddenly stopped me from eating. I was barely eating but was still going to college. I think Instagram can be quite toxic, especially when it comes to communities of young people with eating disorders, such as pro-anorexia forums. I wouldn't say it made it worse, but it definitely played a role. There's a lot of unhelpful content on Instagram, such as encouraging each other to lose weight. I didn't actively or intentionally look at these things but on Instagram you accidently stumble upon this content. That's why it's so dangerous, the content is so easy to access."*

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

The impact of harmful online content on children and young people can be immense.

Ecorys UK's *Qualitative research project to investigate the impact of online harms on children* (2022) looked at how children are exposed to inappropriate content and how exposure to harmful content can promote risky and dangerous behaviour. It breaks down the hazards, risks, and harms of different online content.

The research findings from that work resonate with the NSPCC because they are similar to what we hear through Childline. The NSPCC Learning briefing referenced in previous answers draws attention to the impact of being exposed to legal but harmful content on children (p.5).[1] This includes suicide and self-harm content, online challenges, eating disorder content and pornography.

Legal but harmful content can impact a child's mental and emotional wellbeing; some children told us they were experiencing anxiety, intrusive thoughts, low-self-esteem, and trouble sleeping due to this. Childline insights show that counselling sessions from 2022 –

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

23 which involved discussions of self-harm, suicide, and eating disorder content have more than doubled since 2021-22.

We also know, from our work with the Bereaved Families for Online Safety group, that children and young people exposed to legal but harmful content can be so severely impacted that it contributes to their death. It is important to note that the specific platform or content which is harmful will vary from child to child. For Frankie Thomas, it was the platform Wattpad, a social networking literature site, that "more than minimally contributed" to her death. Whereas in Molly Russell's case, it was Instagram and Pinterest.

Their stories also highlight the need for greater data transparency. Both Frankie and Molly's families have struggled to gain access to data from technology companies which would help the parents understand the impact that content had on their children. In the inquest of Molly Russell, it took the coroner and Molly's family five years to access data from Instagram and Pinterest to understand what Molly was experiencing online before she ended her life. Without greater transparency from platforms, it will be extremely challenging to show the real impact of accessing harmful content and take appropriate regulatory steps to address it.

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

It is unclear if and how services currently assess the risk of harm to children in the UK from content that is harmful to them. We would expect online services to use internal and external data to understand the risks specific to their platform. This should include engaging with children and organisations which represent children to receive an external perspective.

With appropriate transparency, civil society can support online service providers in designing services that mitigate online harms. We expect platforms to use the technologies available to them that assess the risk of harm, including powerful data collection and machine learning analysis tools.

In order to better understand the landscape for child protection, and to provide advice and hold companies to account, researchers, academics and civil society must be able to access the data collected by online service providers on harms and offences identified. The NSPCC and other civil society groups have been at the forefront of raising concerns about online harms through imperfect sources such as internal data streams, counselling helplines, and work with victims.

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

We are pleased that Government has committed to ensuring that platforms publish their risk assessments. This will enable researchers and civil society, as well as Ofcom, to scrutinise the robustness of online services providers' approach to identifying and tackling known and reasonably foreseeable harms. It could also act as a helpful tool for users, and particularly parents, to understand the approach taken by individual companies. We expect Ofcom to provide guidance to the platforms on the format of their risk assessments to ensure they are as accessible and understandable to as wide an audience as possible.

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Is this a confidential response? (select as appropriate)

No

Online services should be considering risks from a range of dimensions including user specific and design feature specific.

User specific

Online services should consider their user base and the different communities within their user base to understand whether there are bespoke risks they need to address. This may include understanding the demographic and interests of users of the services.

In line with a four nations approach to regulation that we advocate in our covering letter, we would expect the Ofcom and platforms to consider the different languages of the UK. For instance, considering whether platforms are placing children which only speak Welsh, Irish Gaelic or Scottish Gaelic at greater risk than children which speak English. According to latest figures there are 384,200 Welsh-speaking children and young people aged 3-24 in Wales. The Welsh Government's Welsh Language Strategy aims to ensure a million Welsh speakers by 2050 and highlights the potential benefits of children being encouraged to use their Welsh language skills socially including through social media. However, there is a dearth of evidence about children and young people's use of social media in Welsh, a knowledge gap that leaves children at risk. Without clear evidence about children's online use in Welsh (or other minority languages) Ofcom will be unable to adequately assess the potential risks and implications for their safety and to ensure that approaches to moderation, reporting and complaints cater to their needs. We would urge Ofcom to work with relevant partners and stakeholders and urgently commission and publish research to build an understanding of the behaviours and needs of Welsh speaking children to inform the development of codes of practice and preparations for implementing the new regulatory framework.

This will be different for each platform, and they must undertake their own analysis.

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Design feature specific

Most online services place a heavy reliance on algorithm to serve content to users. Algorithmic recommendations on platforms such as TikTok work to keep users viewing its content by showing videos based on an assessment of the user's interests.

However, this can introduce unique dangers. A CCDH (2022) report found that TikTok was pushing eating disorder and self-harm content into people's feeds. Following the report, further analysis shows that TikTok had not taken an appropriate response and left many of the harmful hashtags active. TikTok should have taken further action to address this and, if this had happened under the new regulated regime, we would expect that Ofcom would request information from the company and consider both what measures needed to be taken by the company to address the problem and what action they may take as the regulator.

The use of E2EE is an exacerbating risk factor for the safety of children online in the UK. Plans from online service providers, such as Meta, for expanding E2EE risks children's safety.

While encryption measures can generally be seen as a protective layer for sharing sensitive information online, the growing adoption of E2EE by social media platforms can have profound negative impacts on online service providers ability to monitor and report banned content and safeguarding children. The NSPCC's 2021 report sets out these challenges: *End-to-End Encryption: Understanding the impacts for child safety online*

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

Is this a confidential response? (select as appropriate)

No

To ensure child users are safe, we need to create a culture of compliance within online service providers. This needs to start at the top of organisations. Government recently committed to introduce provisions on senior manager liability (SML) into the Online Safety Bill. We now expect to see senior managers being held personally liable for protecting children from harm. Although we are waiting for clarity from Government as to what SML will look like in practice, we would expect governance, accountability and decision making, to flow down from senior management. This should include approval and sign off of risk assessments at the highest level.

We believe that Ofcom should play a role in creating and enforcing a culture of compliance. Other regulators in the UK have taken an active role in ensuring that regulated companies have appropriate governance measures in place. Ofwat sets out the principles of board leadership, transparency and governance that regulated companies

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

must report on. This includes a formalised agreements for Ofwat to meet with all non-executive directors prior to their appointment.

The Health and Safety Executive, which also has SML powers, uses its influence to ensure that companies take their duty of care to protect their employees seriously. T*he Health and Safety at Work Act (1974)* and subsequent case law ensures individual directors and senior managers can be held personally prosecuted for failing to comply with their safety duties.

There must be a culture change across regulated platforms which sees children's safety online as a priority when designing and rolling out services. Whilst it should never be just one person's job to think about child safety, there is a clear need for senior managers to be able to prioritise this issue and have in-depth, expert understanding of child safety and safeguarding. These managers can then hold internal teams accountable for embedding safety by design approaches and, in turn, be held accountable when there are serious failures.

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

Is this a confidential response? (select as appropriate)

No

Please refer to our response to Q5 'What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?' of the previous consultation.

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Is this a confidential response? (select as appropriate)

No

Please refer to our response to Q5 'What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?' of the previous consultation on the first phase.

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

Is this a confidential response? (select as appropriate)

No

The following answer relates specifically to NSPCC's experience of operating as a trusted flagger.

As trusted flagger, the NSPCC has a direct link with some of the online service providers to prioritise content that should be removed. This is used when members of the public share content directly with either of our counselling services, Helpline and Childline, to request take down of content or voice concern about the content.

However, we have recently found issues with this process where an undue level of information is requested from the online service providers, or content has not been removed, even though a trusted body has said this is causing harm. It is essential that online service providers ensure reports from trusted flaggers operate effectively by responding swiftly to content that has been flagged without demanding undue level of information.

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Is this a confidential response? (select as appropriate)

No

Please refer to our response to Q7 'What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?' of the previous consultation on the first phase.

For children to use reporting mechanisms, they need to have faith in the process and this is often not the case. Some young people who have approached Childline said they had tried to report harmful content to platform owners and moderators. Some felt frustrated by this experience, as platforms had been slow to respond and act upon their reports. In some cases, young people had not heard back from platforms at all and the harmful content they were concerned about was still live.

"There's these accounts on TikTok promoting bulimia, anorexia etc. and rating people's bodies. I've tried reporting them to TikTok but nothing's happening. I don't know what more I can do. This kind of content can be so damaging for some people – it makes me sick!". Girl aged 13, Childline.

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

We also hear from young people whose requests to remove harmful content had been denied, as the content in question was deemed not to have breached a platform's community standards.

"I discovered these vile fan fiction stories which described child characters in sexual situations. I tried reporting them to the website, but they said the only way a story could be taken down was if it contained images of child abuse, or if it condoned or suggested the things happening in the story should happen in real life. Apart from that, pretty much anything was fair game. I really worry that children much younger than me might see these stories and become traumatised." Girl aged 16, Childline.

Ensuring that harmful content is taken down from sites is key but it is also vital that this happens swiftly and effectively. Online service providers should ensure that reports from trusted flaggers operate effectively responding promptly to content that has been flagged without demanding undue level of information.

It is important that harmful content reports are fed back into the design of the app, e.g., through algorithms. As seen recently with TikTok accused of ignoring warnings of eating disorder videos, not enough is being done to change and moderate content at a system level. NSPCC support CCDH's recommendations to strengthen content moderation policies and removing a greater number of harmful hashtags.

As Ofcom will be aware, the NSPCC has been working with organisations across the women and children's sector on a *Violence Against Women and Girls (VAWG) Code of Practice.* In that we set out that services should adopt the following reporting measures:

- Users must be able to effectively report content that is illegal or harmful to regulated services through clear and transparent flagging mechanisms. Regulated services are obligated to have effective and easy to use reporting functions and must use them to triage content for both human and automated moderation.
- Service providers should have reporting processes that are fit for purpose for reporting child abuse content and wider harms, that are clear, visible and accessible and age-appropriate in design. Thought should be given to reporting avenues for non-users such as teachers or family friends and support services, who are able to report without the victim needing to engage further with the harm.
- Service providers should have in place clear, transparent, fair, consistent and effective processes to review and respond to content reported as child abuse or harmful content. Users must be given the ability to submit third-party content to the companies' intelligence systems in relation to specific cases of content violation.

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Is this a confidential response? (select as appropriate)

No

Please see our response to Q18 "Are there any functionalities or design features which evidence suggests can effectively prevent harm and could or should be deployed more widely by industry?' in the previous consultation on the first phase.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

Is this a confidential response? (select as appropriate)

No

Please refer to Q18 "Are there any functionalities or design features which evidence suggests can effectively prevent harm and could or should be deployed more widely by industry?" in the previous consultation.

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Support to children exposed to harmful content
Services should provide support to children and young people exposed to harmful content on their platforms, particularly following reports from children which flag harmful and inappropriate material. This could include signposting them to support organisations. We would suggest that online services engage with support organisations before directing a significant number of users to the support service to ensure that they can cope with the additional demand.

Multiple methods of reporting

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?
Online service providers should be offering multiple accessible reporting options to children. Online service providers should also be doing more to highlight different options, such as muting, which could play a vital role in young people's friendships online. These reporting systems need to be accessible, usable, and meaningful so that users are encouraged to report harmful content they come across and reassured that it is being dealt with. **Cultural change in reporting harms** Online service providers have a responsibility to tackle the normalisation of online harms. Reassurances over anonymity and confidentiality should be offered as much as possible. Online service providers need to take a victim-centred approach to dealing with reporting and complaints mechanism.

Annex – CONFIDENTIAL [4 May 2023]

Separately to our full response, we also wanted to share insight from a young person who is a member of the NSPCC's Young People's Board for Change.

The Young People's Board for Change have played an active part in informing the NSPCC's influencing on the Online Safety Bill and our wider Child Safety Online strategy. One of the members reached out to us due to their concerns about the social media app Snapchat, and the risks it poses to young people. These risks cover the spread of both illegal and legal but harmful material on the platform.

The insight is particularly relevant to the consultation questions about harmful content online (Q6), exacerbating risk factors (Q9), and reporting and complaints systems (Q13 and 15). It is also just one example of why it is vital that children are heard in the new regulatory framework. Children and young people are experts in their own lives and have direct insight into the realities of being online that are vital for decision makers to seek out, hear, and act on.

To ensure children are heard, Ofcom must have permanent lines of communication with the children's sector. As Ofcom will know, the NSPCC is calling for user advocacy arrangements for children to be introduced in the online safety regime. We believe this is the best way to ensure that children's voices and experiences are considered by decision makers.

The insights and the identity of the young person are confidential and must not be shared publicly. We would be happy to organise a meeting between Ofcom, Becky, the young person who shared this insight, and the NSPCC if that would be helpful.

If you have any questions or would like to discuss this insight in more depth, please contact us via rani.govender@nspcc.org.uk.

Insight shared by Becky (aged 17) regarding Snapchat

- **'My Eyes Only'**
    - Snapchat has a 'My Eyes Only' section, which enables users to save Snaps and Stories in a password-protected folder on the app. Becky noted that having a 'My Eyes Only' folder with a password indicates to young people that

they can use this for images that they do not want shared with anyone else. This can lead to young people uploading images which put them at risk if shared.
    - Becky knows of multiple young people (under 16) from her community who have had their accounts hacked and images from their 'My Eyes Only' folder shared publicly on Snapchat, including intimate images.
    - Even in cases where these images have later been removed, other users have had the opportunity to screenshot them. It is not possible for the user to know who has seen these images and who has saved them.
    - Becky questioned why this feature exists for under 18 accounts, considering the behaviour it encourages and the potential risks it exposes to young people using it. In her experience, it has indicated to young people that it is a safe folder and that private images should be uploaded to the platform.

- **Community Guidelines**
    - Following intimate images being leaked from the account of another young person (aged under 16), Becky reported seven of these images to Snapchat. Snapchat responded to say that only one of the seven images broke their Community Guidelines, despite them being of someone under 16.
    - The images were later taken down, although Snapchat did not assist with this process. Becky has highlighted that there is a significant issue with semi-nude and nude images of young people under 16 not being removed from Snapchat despite being reported, even if a young person is in underwear and has had the image shared without their consent.
    - In comparison, Becky noted that other apps such as TikTok and Instagram are much more responsive when blocking intimate images of young users.

- **Age verification**
    - Becky called for apps such as Snapchat to have stronger age verification systems. She notes that young users are easily able to circumvent age assurance measures on a lot of platforms, and as a result they do not have the necessary protections in place online.