Your response

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

Response:

Ukie is the trade body for the UK's video games and interactive entertainment industry. A not-for-profit, it represents more than 600 games businesses of all sizes from start-ups to multinational developers, publishers, and service companies, working across online, mobile, console, PC, esports, virtual reality and augmented reality. Ukie aims to support, grow, and promote member businesses and the wider UK video games and interactive entertainment industry by optimising the economic, cultural, political, and social environment needed for businesses in our sector to thrive.

Ukie's members appreciate Ofcom's careful consideration of the potential causes and impacts of online harms and the cumulative impact of the proposals in addressing those identified harms, and we are aware that these proposals can't be one size fits all as Ofcom considers over 100,000 services.

Our response reflects the fact that our industry considers the safety of our player community as paramount. There are over 3.4 billion players globally, and Ofcom's recent Online Nation 2023 survey found that 38% of UK adults and 57% of UK children reported playing games online. The industry is committed to creating a safe, fun, fair and inclusive playing experience for this large and growing audience, and to provide the information and tools necessary to allow parents, carers, and players to customise their own experience and set their own boundaries.

It is a business imperative for games companies to provide safe, welcoming places for their customers to play together online. In such a highly competitive global market, players who do not feel safe always have many options for other games to play – often entirely for free. Any game which develops a reputation as unsafe will quickly lose its audience.

As a result of these priorities, the video games industry has a long track record of spearheading self-regulatory efforts. Our industry has long provided parental controls on all major platforms, implementing the PEGI system of age ratings, as well as funding consumer information campaigns on how to play safely online.

As an industry, we take our responsibility to players of all ages seriously. Our commitment is structured around the following pillars: (i) age-appropriate pre-contractual information, (ii) safety by design in online environments, (iii) tools to enable players, parents, and caregivers to set the permissions that are appropriate for them or their children, and (iv) enabling consumer redress and efficient and proportionate enforcement.

In addition to the requirements stipulated by law relating to pre-contractual information to consumers, in 2003, the video game industry established the PEGI system of age ratings across Europe. PEGI operates through a set of scientifically backed ethical standards in the form of a Code of Conduct. Since 2012, PEGI has a legal basis in the UK where its administrator, the Games Rating Authority, provides statutory rating of video games in line with the Video Recordings Act. The PEGI system is a central part of our industry's commitment to protect minors and behave responsibly, especially where children are concerned.

It is important to mention that online multiplayer games vary greatly from social media and other online platforms. Content is designed to meet our well-established age-appropriate standards, and where interactions between users are possible, they will typically be limited in nature, often ephemeral, and restricted by parental controls or according to the age-appropriateness of the product in which they are contained.

As a result of this long-held determination to combat illegal content, and more broadly unacceptable content, within our services, combined with the inherent safety-by-design nature of interaction within video games, we believe that our sector is at a lower risk of hosting illegal content than many other online sectors.

We understand the importance of assessing the risk of potential online harms, however, we are equally concerned that if a reasonable balance is not struck, then this requirement will be burdensome for our members, including the numerous start-ups, Micro and SMEs which make up approximately 99.5% of our sector.

Our members therefore call on Ofcom to make proportionality the central focus when developing the guidance, considering the differing nature and functionalities of services and user interaction across our industry, as well as the existing mitigation methods the industry has championed for decades. As we argue in our answer to question 7, risk assessments must take into account 'how the design and operation of the service (including the business model, governance and other systems and processes) may reduce or increase the risk identified. Given the complexity of some games and the complexities of an industry which publishes across multiple platforms, delivering multiple ways to experience the content, we are concerned the burden of the task, particularly for the Start-ups, Micro and SMEs which make up a significant portion of our sector, may be unmanageable.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Response:

We are concerned that the consultation documents show a misunderstanding of the nature of video games services and the risk levels they are likely to represent for dissemination of illegal content.

The only references to video games can be found in the guidance on Risk Assessment (Annex 5 Guidance - Type of service on page 54) which states that video games are at an increased risk, without providing any evidence. Ofcom implies the level of risk based on unvalidated assumptions

– see Volume 2 “Second, we do not have specific evidence relating to all types of U2U services. There is more research available - including on risks of harm to individuals - about large social media sites, gaming sites, and services that publish public information that can be analysed. Where appropriate, we have made reasonable inferences about the risks that may arise on other services where we do not have specific evidence about that service type.”

The available evidence base, and our members’ combined experiences, make clear that our industry sees significantly lower rates of illegal content sharing than many other online services. For example, services available in the United States (effectively all online services) are required by law to report all instances of CSAM and grooming material they detect to the National Centre for Missing and Exploited Children (NCMEC). In their Cyber Tipline report 2022, which set out the reports received from all services, they revealed that out of 32 million total reports, only 8200 reports were from video game platforms. That represents approximately 0.00025% of the total reports received by the NCMEC Cyber Tipline in 2022. It would therefore be disproportionate to equate the risk of CSAM appearing in video games with the risk of such content appearing on other online platforms, such as social media. This greatly reduced risk should be reflected in the guidance and in the risk profiles that apply to video games.

The games industry is a leader in keeping players safe online. The industry has well established practices to protect players and it has been leading on this front for decades with effective, industry-led measures to protect all users, and particularly younger users. This includes work across a series of initiatives and partnerships, such as: with the National Crime Agency and NCMEC to combat online abuse and CSAM material, the creation of the Pan-European Game Information (PEGI) system, active membership of the UK Council for Child Internet Safety, and Ukie’s domestic Get Smart About P.L.A.Y campaign, first founded in 2020.

All game platforms and game publishers have robust terms of use that set expectations for safe and inclusive behaviour and which they apply to discipline against disruptive play. This is in addition to technical safeguards such as content filters, reporting mechanisms, and dedicated moderation teams which work together to provide one of the safest and most sophisticated online environments for our players. Additionally, the safeguards are supported with well-developed enforcement policies, enabling companies to remove offenders with temporary or permanent bans, in a proportionate manner. The video games industry has decades of experience in creating online spaces in which players choose to spend their time because they are welcoming and safe.

Underlying all of this work is the very nature of interaction and communication within games. Our members do not provide spaces for people to hold long conversations, share videos and photos, and generally communicate with the outside world. Communication within games is typically ephemeral, to limited and changing audiences, and of a restricted nature. The possibility to share illegal content is often very restricted merely by the design of the service. The comments in the consultation documents indicate that Ofcom has not yet understood this.

We hope that throughout this consultation we are able to provide evidence on the well-developed safety practices across our industry and we look forward to engaging with Ofcom in the future to improve their understanding our sector.

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 2:	
i)	Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.

Response:

The consultation does not properly explain how service providers can consider the different functionalities, contexts and types of user generated content (UGC) that they may enable as a factor in determining the level or risk of illegal content harming users of the service. It does not give enough space to consider safety by design, in effect. We argue that this is an important consideration that should be taken into account.

With respect to the type of UGC shared and how in games, the following specifics are noteworthy:

1. Usernames/Profile Pictures/team names – low risk of this type of content being illegal content, even though visible to all users and are persistent. All major developers have robust and swift processes in place to automatically detect, block, and remove offensive usernames.
2. Text/voice chat – this type of UGC is often session based and differs between lobbies/groups (multiple users likely to be strangers) and parties/private messages (limited number of users likely to be friends); voice chat sessions are usually ephemeral/session-based and can't be recalled, reposted, commented on etc. The purpose of the communication is also inherently limited – people are talking to make decisions about their gameplay or collaborate as a team, not to share broader information. This creates far fewer opportunities, or reasons, to share illegal content.
3. Images/videos – it is important to distinguish between in-game assets (anime, cartoon, computer generated) that can be shared and real photos/videos uploaded to the service; the latter are far less common in games. A service with image or video sharing which is more persistent may increase the risk of illegal content, but only where the photos/videos shared include real photos/videos as opposed to in-game assets. The associated obligations with respect to mitigating the risk of illegal content should be reasonable and acknowledge that fewer mitigations would be expected of services that only allow users to create and share UGC using in-game assets given the greatly reduced risk of illegal content being involved. Similarly, where a service subjects all uploaded images/videos to mandatory review prior to being made available in the game, it should be acknowledged that such review greatly reduces the likelihood of any illegal content being present in such uploaded images/videos.

As acknowledged by Ofcom in recent industry roundtables, the risk profile of a service should be capable of being impacted by the mitigation efforts implemented by the company responsible for that service, particularly where, for instance, changes in the data relied on to determine the

service's risk profile can be observed after additional safety measures are implemented. This very important fact needs to be more clearly set out in the guidance. The guidance on assessing risk is very convoluted and seems to set a very high bar for a low-risk service, services that do not have a large number of UK users, or companies that release multiple services every year.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:
i) Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response: NA
ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 4:
i) Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response: NA
ii) Please explain your answer.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 5:
i) Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response: NA
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response: Tying remuneration for senior managers to positive online safety outcomes could, depending on how the proposal is structured, have a chilling effect on the willingness of individuals to take on such roles. Online safety outcomes are not determined by a single person, they are determined by a myriad of employees, contractors, and vendors all working towards a common goal as well as by the users of the service and how they choose to interact with one another on the service. Tying an executive's remuneration to positive online safety outcomes misunderstands how trust and safety compliance programs operate and disproportionately assigns responsibility for negative outcomes to executives who are unlikely to have had a significant role in the implementation or day-to-day management of programs.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Service's risk assessment

Question 7:	
i)	Do you agree with our proposals?
Response: The assessment of risk should take into account the nature of the service, and specifically the type of communication that can be done via that service and the mitigation measures adopted by the company responsible for the service, as well as the types of illegal content that could potentially be shared. Any service that allows the sending of text could potentially be used to send almost any illegal content (except pictures, voice, and video), but what is actually capable of being shared can differ wildly depending on the nature of the communication functionality and the mitigation measures implemented by the service provider. Specifically, the communication capabilities in games are usually far more restricted than the capabilities in social media platforms. It is almost invariably ancillary to the core features of the service. Unlike social media, the purpose of the communication is to enable, enhance or complement the gameplay. Games services are not there to provide open forums for sharing of ideas and long-term conversations about topics outside of the game. The purpose is purely to discuss the gameplay. The communication is often limited in many ways as a result, such as by the amount of text that can be shared, or the number of recipients. In many cases it is not possible to choose recipients, or to find the same recipients again for continued conversation on a later occasion. Interactions are often session-based, with a purpose to collaborate on moment-to-moment gameplay, not to develop long-term conversations about broader topics. It should be made clear in the guidance that games providers are allowed to assess how feasible it is for any meaningful amount of illegal activity to take place on their services in determining	

whether their services are low risk, multi-risk or high-risk. Past experience of running that service, or similar services, should be an important factor in this. Many Ukie members report that they have exceedingly rare instances of illegal content in their services. To suggest that they are 'multi-risk' services, and therefore automatically medium or high risk, because it is technically possible for more than one type of illegal content to be spread, without simultaneously considering the mitigation measures that may have been adopted by the service provider, is disproportionate and makes the assessment process redundant.

The goal of the risk assessment process should be to assess the actual risk of illegal content appearing on the service in question, not the risk of illegal content appearing on the service absent any mitigation measures. If that were the case, the risk assessment would not be of the service in question, but of a different service entirely. The risk assessment process, if it is to be suitable and sensible, should be used to help companies understand where they may need to focus more attention in order to mitigate the residual risks to their users that are presented by their services. If those actions are taken, then companies should be able to adjust their risk assessments accordingly. This should be more clearly and prominently set out in the guidance.

Similarly, when determining the risk level of an identified harm, it should be clearer that an isolated example of the identified harm materialising on the service should not mean that the harm is automatically deemed to be medium or high risk. For instance, the grooming decision framework for assigning risk levels suggests that a service will automatically be deemed medium risk for grooming if children are able to access the service and communicate one-on-one with other users and there is **any** evidence that the service has been used by offenders for the purpose of grooming. The guidance should acknowledge that such evidence may only indicate that the service may be medium or high risk for grooming, but that that initial indication may not be appropriate when considering the totality of the evidence at the service provider's disposal. There should be an appreciation of factors such as the frequency of such examples arising, the proportion of the total number of complaints received by the service provider that relate to such harm and that are verified by the service provider as evidencing such harm, and the mitigation measures that have been implemented to reduce the likelihood of such harm arising. It would be perverse for a service to be deemed medium or high risk, and therefore be subject to the additional obligations that flow from that designation, simply because of an isolated incident.

Given the complexity of some games and the complexities of an industry which publishes across multiple platforms, delivering multiple ways to experience content, we are concerned the burden of the task, particularly for the Start-ups, Micro and SMEs which make up a significant portion of our sector, and those companies that develop and publish multiple games every month, may be unmanageable. If services are similar to previously published services, then absent any material evidence to the contrary, it would seem proportionate for service providers to be able to utilise a single risk assessment for multiple services with the same functionality and same mitigation measures implemented, particularly where such services are not Large Services for the purposes of Ofcom's guidance.

The obligations outlined in the guidance are effectively a one size fits all, and do not accommodate the real differences between social media platforms and online games with user generated content (UGC) in terms of how the services are used, the type of UGC shared, and the permanence of the UGC and its impact. The Australian Online Safety Act and the European Union's Digital Services Act distinguish between different types of services and set differing compliance requirements according to the risks presented by both. U2U services are not distinguished by the type of service they are, i.e. what is the primary functionality of the service whereas such a distinction is made in the EU's DSA. We would recommend that if there is no sharing of UGC, the obligations should not be as

stringent given the level of risk overall is lower because of the limited nature of the exposure to that UGC. In conclusion: greater clarity is needed for companies that their assessment can include consideration of the nature of interaction between their users, the functionalities that are available, the types of communication or content that can be shared, and their past experience with the amount of illegal content, if any, that is shared on that or similar services they have run.
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:
i) Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response: The threshold for carrying out a new risk assessment is unworkable. The 'significant changes' that Ofcom describes (adding or removing functionalities, updating product policies, updating the design of user-facing functionalities, changing growth strategies) are part of the day-to-day pace of how UGC services operate and innovate. The risk assessment process set out by Ofcom's guidance is far more complicated and onerous than the DPIA process – Ofcom's own timelines indicate that the Illegal Harms risk assessments will take three months to complete. Requiring services to carry out entirely new risk assessments before making the kinds of changes described in the consultation, in addition to the annual risk assessment, is completely infeasible – services would be in a constant state of creating new risk assessments, which would likely be out of date quickly when a new policy or feature launches. Ofcom could consider making the risk assessment process lighter and less resource-intensive, or changing the requirement so that services need only update relevant portions of their existing risk assessment, rather than having to carry out an entirely new one. Additionally, due to the length and complexity of the guidance, we would recommend creating visual and easily digestible explanations of how companies need to engage with the final process.
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response: The overall Risk Profiles are clear. However, we would like to highlight that the guidance is not clear on defining the scope of a service for which a risk assessment needs to be carried out. It is crucial for our members to have clarity on whether they would need to carry out a risk assessment for every video game they develop, for every platform version of every video game they develop, or simply one risk assessment per company or genre of game. We think the approach should be aligned with that of the PEGI system, which operates through a set of scientifically backed ethical standards in the form of a Code of Conduct to provide pre-contractual information to consumers on the contents of a game, and only requires one risk assessment per platform. Since 2023, the new PEGI Code of Conduct forces companies using PEGI to adhere to online safety standards. Ukie also acknowledges Pegi as best practice. The issue of the definition was raised directly with Ofcom during roundtables, and we were told that Ofcom will look into this issue. Ukie and the whole video games industry is readily available to provide more evidence on this matter.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response: NA	
iv)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12:
i) Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response: There is a universal commitment across the video games industry to provide safe, fun places to play online with other people. All companies have clear terms of service and act to remove any content or interaction which breaches those terms, including any illegal content. The video games industry has a long track record in spearheading self-regulatory efforts to address this as set out in this response, from introducing parental controls on all major platforms to funding consumer-facing information campaigns on how to play safely online. Our industry is one which is built on innovation, with a diverse range of business models and evolving products. Content and business models aside, there is also a myriad of ways in which the products are experienced and delivered across multiple platforms. Most members that host U2U services have rules that prohibit more than the specific types of illegal content as defined by the Online Safety Act. They try to ensure that the content displayed on their platform is not only legal, but also appropriate for users. The Community Standards of most game developers describe the type of content they find objectionable, and they take various measures to mitigate the risk of such content being made available to their users. The nature of online interaction within games is nuanced and specific and must be considered when considering online harms. Consideration must also be given to the global nature of many of the platforms and services in our sector. Developing regulation that acknowledges the nature of global businesses and is consistent with the expectations or regulations of other countries is essential.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 13:
i) Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?
Response: Please see our responses above regarding how services are designated as medium, high, or multi-risk services. As a general matter, our members support the principle that compliance burden should be proportionate to both the service's size and resource levels, and the risks they pose.
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 14:
i) Do you agree with our definition of large services?
Response: While we understand the comparative analogy to the DSA deployed by Ofcom in setting the threshold for 'large' services, we do have some concerns about Ofcom's proposed definition of large services and its corresponding implications. Rather than arbitrary thresholds, the focus should be on the functionalities of the service and the overall risk profile that is presented to users. Additionally, our members would want Ofcom to clarify if the average monthly user base is active or registered users as this was not clear in the documentation. If active, how should this be measured? Would merely accessing the service be enough, or would there need to be some form of actual engagement with the service beyond just accessing it?
ii) Please provide the underlying arguments and evidence that support your views.
Response: We agree that the impact of the law should be focused on those services which pose the most risk of British citizens being exposed to illegal content online. However, we have concerns with Ofcom drawing parallels to the EU's Digital Services Act (DSA) in setting the threshold for 'large services. While we understand the reasoning behind mirroring the DSA's approach, we have several observations and concerns regarding its application in the UK context. One such observation is that the scope and nature of online services vary greatly. Simply mirroring the DSA's user base threshold might not adequately reflect the diverse risks and responsibilities associated with different types of platforms in the UK landscape.

Additionally, user base size is not necessarily determinative of, or the most appropriate proxy to, whether it is justified to impose more onerous measures for some services. Therefore, applying prescriptively Ofcom's 'large' service definition to mean 'service deserving of more measures' can lead to disproportionate results and unfair outcomes in some cases.

To effectively assess online safety risks and responsibilities, Ofcom needs to move beyond a one-size-fits-all approach and embrace the multi-faceted framework offered by the DSA analogy. This will ensure fairer regulations that address the diverse realities of online platforms and ultimately keep users safer.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Question 15:

i) Do you agree with our definition of multi-risk services?

Response:

We do not agree. We think the definition is too restrictive and disproportionately impacts games companies due to the nature of their platforms.

Following extensive consultation with our members and legal services, we are concerned that, by virtue of the way the guidance is currently drafted, any game company whose U2U service includes chat functionality would almost invariably be deemed to be either a high risk or multi-risk service merely due to the existence of that chat functionality. It is very difficult to see, in fact, how any service that features some kind of user interaction can be deemed low risk under these proposals.

This, in return, would result in services finding themselves in the multi-risk category despite not actually presenting the level of medium-high risk that would warrant the more burdensome obligations associated with the multi-risk designation.

A more proportional approach to the multi-risk assessment is needed, determined by viewing historical data, how the service is used, and the types of UGC shared, as well as any mitigation efforts, rather than a tick box exercise. It is not currently clear why only two identified medium risks should result in a service being deemed to be a multi-risk service, and not say five identified medium risks or two identified high risks. It would be fairer and more proportionate to introduce some middle ground between services that only pose a risk of two types of illegal harm and those that pose risks of nearly all of them – and to take into account how significant the risk of each of those types of harm is in light of the actual functionalities of the service.

Ofcom's current approach also treats all illegal harm as being equal. A service that is at high risk of terrorism and CSAM is treated in the same way as a service at medium risk of drugs and proceeds of crime offences, whereas the criminal law would treat the respective offences very differently, recognising their different levels of severity and the harm they cause. The Online Safety Act addresses this by asking services to prioritise based on potential harm. Section 9 requires considering the nature and severity of different illegal content, while Section 10 emphasises effectively mitigating these risks. Given limited resources, services can prioritise based on potential consequences, directing efforts towards mitigating harm with the highest potential for severity. We consider it is appropriate for services - and consistent with sections 9-10 of the Act - to prioritise resources addressing those harms that have the potential for the most severe consequences for individuals.

ii) Please provide the underlying arguments and evidence that support your views.

Response:

Proportionality of scale and type of risk must be a key factor when considering appropriate responses and measures for online businesses. The games industry is diverse with businesses of all

sizes creating and publishing content across multiple platforms. This is true of the wider tech sector. We have mapped over 2,600 games companies located in clusters across the UK. We are home to global publishers, platforms and many development studios including large and medium sized companies and a wealth of small and micro independent businesses. The diversity of size and type of business in the games sector means a one-size fits all approach to online safety would not be effective and we welcome the indication that proportionality, feasibility, and ability to apply the code of practice will be respected.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 16:
i) Do you have any comments on the draft Codes of Practice themselves?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 17:
i) Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: Our members agree with the proposals and would like to note that content moderation has been an integral segment of every video game providing U2U functionality. The below hopes to provide an overview of content moderation already present in the industry, providing examples of best practice, something Ofcom has asked the industry to provide as part of our response. The games industry is a leader in keeping players safe online**.** The industry has well established practices to protect players and it has been leading on this front for decades with effective, industry-led measures to protect all users, and particularly younger users. This includes work across a series of initiatives and partnerships, such as: with the National Crime Agency and NCMEC to combat online abuse and CSEA material, and Ukie's multi-year domestic Get Smart About P.L.A.Y campaign.

The PEGI age rating, which is a requirement by all the major platforms and publishers, has its own strict rules for content moderation, reporting and content removal that all PEGI signatories must follow. PEGI also independently monitors and enforces compliance, meting out monetary fines and/or sanctions as required.

All game platforms and nearly all game publishers have robust terms of use that set expectations for safe and inclusive behaviour and which they apply to discipline against disruptive play. This is in addition to technical safeguards such as content filters, report mechanisms, and dedicated moderation teams which work together to make the experience of players one of the safest and most sophisticated online environments. The video games industry has decades of experience in creating online spaces in which players choose to spend their time because they are welcoming and safe.

Proposals that would prioritise content for review are not fit for purpose for most members, as with U2U services or in-game communications do not lend themselves to the time sensitive issues of virality or public engagement on pieces of content.

In addition to the above, members often collaborate with safety organisations and other platforms that focus on child safety and internet safety including the WePROTECT Global Alliance, the Internet Watch Foundation (IWF), the UK Safer Internet Centre, Fair Play Alliance, Family Online Safety Institute (FOSI), Digital Wellness Lab, Connect Safely, and kidSAFE among others.

Additionally, games companies often share learnings and development efforts with the industry and the wider technology sector, meaning they work closely with other chat, social media, and UGC (User Generated Content) platforms to report bad actors and content, so they can also take appropriate action on their platforms. In consultation with expert organisations such as the Anti-Defamation League, Tech Against Terrorism (TAT) and The Simon Wiesenthal Center, as well as academics and safety partners from across the globe, game companies are constantly evaluating their moderation policies and are proactively seeking to learn from and implement industry best practice.

Companies also frequently audit their games and content moderation functionalities to ensure they are continually strengthening their processes and algorithms to prevent, detect, and block new content or behaviour that violates their Terms of Use. If any users are found to be violating these standards, they may be suspended or removed from the platform. In some cases, companies also work proactively with authorities to report cases of violent threats, child endangerment, or other serious real-world harm.

The methods of content moderation vary between games companies depending on their size and products. The below presents a further example of the content moderation methods used by some companies who develop large online multiplayer games:

Filtering

Most online multiplayer games have built-in, automated and proactive moderation, algorithms and tools designed to automatically protect Users by detecting and filtering out illegal and harmful content before it is published. This includes:

- Keyword filtering, being profanity filters which automatically identify and block certain content.
- AI filtering (text, graphics and voice), being artificial intelligence technologies to monitor, analyse, and moderate content.
- Anti-cheat software.

Reporting

If a User or other individual/entity identifies content or behaviour which they consider offensive or potentially illegal, Users can submit a report to the company:

- in the Game itself via the Customer Service button accessible from the main menu, or
- outside of the Game by contacting the developers Support Email Address.

Moderation

Once a company becomes aware of any content that is a potential breach of their terms and conditions, (via their algorithms or a report), they have a dedicated team of personnel to assist in reviewing such possible violations and in determining what enforcement action should be taken. That includes whether the content is illegal and requires escalation to law enforcement. They may also utilise automated technology to categorise certain violations.

On receipt of a report, the moderation team aims to take any required actions (see Enforcement Actions below) as soon as possible, although the period required may be longer where the report is more complex or during peak support periods close to a new game's launch or a significant content update.

Enforcement Actions

Where content moderation teams have detected content in the game breaching their terms and conditions, they will remove such content from the Services.

Restrictions may be imposed on users for breaching terms of service. These restrictions will often be determined by the moderation or support team acting in a diligent, objective and proportionate manner, taking into consideration the severity of the breach and any previous violations committed by the user. These enforcement actions include one or more of the following:

- The User may receive a warning: Users may receive a warning from the company informing them of their breach and putting them on notice that carrying out further such actions may result in them receiving a harsher enforcement action.
- The User's content will be removed: As set out above, if the company find a User has uploaded or transmitted illegal content, that content will be removed from the Services.
- The User's account may be suspended or restricted. Where a breach is deemed more severe, or where a User is carrying out repeated breaches of their Conduct Rules, the User may have their account suspended, or be subject to restrictions on their account.

- The User may be banned. For the most severe breaches, or where a User is carrying out repeated breaches of the Conduct Rules, the User may have their account permanently suspended. For some console makers, in the event of a serious violation, not only will the account be permanent suspended, but they will be prevented from connecting their console to the networks, placing a financial barrier between the offender and their ability to rejoin.

Additionally, a crucial aspect of content moderation is the position of community manager. They serve as the direct link between a company/product and its players. They relay the perceptions, expectations, trends, and any other important information about the fans directly to the company. They also foster the community by giving them things to talk about and content to enjoy/critique. Online community managers have their origins in the games industry dating back to the original MMORPG games as early as 1995. The roles vary vastly from company to company and different specialist skill sets are needed in different companies.

Community teams for some larger games companies are starting to introduce semantic analysis tools to assist community mangers in identifying warning signs earlier in game play and are regularly collaborating with charities to ensure vulnerable young people are able to access the help they may require.

ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Content moderation (Search)

Question 19:
i) Do you agree with our proposals?
Response: NA
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Automated content moderation (User to User)

Question 20:
i) Do you agree with our proposals?
Response: Most systems used to moderate in-game communications and UGC are proprietary tech. Companies currently use a mixture of automated and manual processes. Some systems also have a dependency on Analytics Team (ADSE) workflows, ADSE may use external software, data storage and similar, not explored here. The games industry employs a large number of tools, techniques, communities and moderators to safeguard users and maintain their games experience. Individual companies will have their own methods which will be appropriate to their own game rather than there being a generic solution or set of tools. Due to the commercial sensitivity of these proprietary tools, we are unable to list specific examples in this paper. Increasingly, machine learning is being used to enhance and improve moderation of in game communication and is now able to cover images, text, and audio. As machine learning become increasingly more sophisticated, games companies may be provide richer and enhanced monitoring to support the human moderators not only to cover more content but to identify new and emerging threats at speed. Auto-moderation and the use of machine learning to monitor online spaces does not replace the role of highly trained and specialist moderation teams, but instead enhance the capacity and effectiveness of safeguarding. Through machine learning and natural language processing algorithms, some games companies are able to identify and hold potentially problematic content from player interactions (such as chat functions), or to have certain interactions flagged for review and potential enforcement action against the responsible players.

At a high level, members utilise various tools to filter out banned words, phrases and URL addresses, filter player abuse reports for key trigger words which can then be manually reviewed by content moderators, scan chats for child exploitation, harassment, and risks to life, and review images uploaded to the service for possible violations of their terms of service. Automated systems also play a key role in detecting cheating or highly toxic players.

Companies will routinely offer a complaints process, allowing people to challenge findings that they have committed a breach of terms or illegal activity against other users.

All moderation services and approaches are agreed with product and content moderation teams, and any process with game account impacts are also regularly sampled to sense check effectiveness and identify false positives so that the processes can be edited and improved if required.

ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 21:	
i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response: The guidelines generally aim to recognise the variety of services users may engage with. Many gaming companies also remind players through Codes of Conduct, Community Guidelines, etc that they should not consider messages to other players as "private", or confidential.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response: Accuracy can vary depending on hash distance settings and additional filters. The costs of applying CSAM hash matching include start-up engineering, training and labour costs, as well as to apply the human review to all flagged reports.	

ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 23:	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response: Main challenges for member companies when implementing measures were associated with engineering and labour costs to adapt their procedures, technology, and teams to meet external databases.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response: As noted above, the main costs for members are associated with engineering and labour costs. For many of our members, their experience is that the prevalence of CSAM URLs being shared on their networks is low, limiting the value of fuzzy matching for CSAM URL detection.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response: There is significant cost in engineering and labour for our members.	

ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	
Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response: Mostly, except for the proposal that filtered content should be restored upon successful appeal, as this is not practically possible in many circumstances. Due to the ephemeral nature of communication within a game, filtered content cannot be put back in front of other users later on. Another concern members raised is on the proposal of providing indicative timelines for deciding the complaint. Members believe it is not the right, or indeed most efficient way, and instead propose to allow the user to access a tracked status of the report. They believe that the latter method would empower the user with more relevant information.	

ii)	Please provide the underlying arguments and evidence that support your views.

Response:

Player reporting remains a critical tool in how games companies promote safe gaming spaces, allowing players to flag disruptive behaviour so that moderation teams can investigate it (see answer to question 18). Most online multiplayer games launch with in-game reporting for disruptive or inappropriate behaviour. Reporting tools should be accessible - but also thorough – that have enough steps to ensure clarity, accuracy, and information for teams to review, and deter bad actors. Companies use a combination of technology and human moderation to review player reports.

As stated in our answer to question 18, content moderation teams which detected content in the game breaching terms and conditions will remove such content from the Services.

Filtered content: Ukie members have raised concerns about the proposed requirement that all filtered content be restored automatically in the case of a successful appeal. This will often not be practical to do in real time, as interactions within games or services are ephemeral. Companies may instead work with users to update and improve filters so that the same text, image or other content is not caught by the filters in future, allowing players to re-upload.

On the **indicative timelines**: While providing indicative timelines for complaint decisions offers transparency and accountability, some members raise concerns about their inflexibility, potential for missed deadlines, and reduced decision-making power for complaint handlers. At least one of our members finds that enabling users to check the status of their reports is a better alternative to providing indicative timelines. User reports are generally prioritised and handled differently depending on a number of factors, including severity of harm and likelihood that the content is illegal (as Ofcom recommends in its U2U content moderation Codes). For platforms that host multiple modalities of content across numerous surfaces, providing a reliable and consistent estimate for reporting turnaround is difficult and likely to result in a less satisfying user experience.

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No.

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response: Given the OSA's info requirements in the terms of services are incredibly detailed and very specific (e.g. requiring separately addressing each form of primary priority content that is harmful to children) the information will certainly be very long and the most detailed section in many of our members terms of services. This will have the overall impact in making providers terms of services even longer and more unwieldy for users. This is contrary to the OSA's aim to ensure that terms of services should be drafted in a way that minors can understand the content. Minors, and the majority of users, will have difficulty of understanding a long document that will necessarily also include other rights and obligations, e.g. boilerplate clauses, IP clauses liability clauses etc. A better solution would be to allow providers more flexibility in including the OSA's info outside of the terms of services on their website. For example, Safety pages, articles, etc allow for varied mediums of presenting information (icons, videos, text) that can be more accessible for users of different ages and accessibility. As well, the ability to include a URL in the terms of services to a webpage containing the required info in the OSA would be a preferable way of meeting the OSA's information requirements.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Default settings and user support for child users (U2U)

Question 31:
i) Do you agree with our proposals?
Response: Our members agree with the need to constantly innovate and provide greater protection and safety for child users. However, we want to ensure that these proposals do not hamper the ability for real life friends seeking out each other and connecting online. For our members, many games allow for online match making, either to build teams, or partners for a specific game. It would be important to clarify the definition of "prompts to expand their network of friends", to ensure that it is limited and does not include multiplayer games where someone can join. If this is applied broadly in that case it would make it impossible to have multiplayer online games with other players. As well, not including players in publicly visible lists makes any interaction difficult or impossible, even if they are part of a team. Chat or communications controls can help to ensure the same outcome without impacting the overall experience that a group of friends may be looking to experience.
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 32:
i) Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response: NA
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response: No. For game companies, the limited prevalence of illegal content does not warrant it.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response: NA	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:
i) Are you aware of any other design parameters and choices that are proven to improve user safety?

Response:

Yes. See below.

Yes. As mentioned previously, the PEGI system is successful in establishing good practice. Each publisher that joins PEGI has to sign a Code of Conduct committing them to provide users and parents with objective, intelligible and reliable information regarding the suitability of a game's content. By signing the Code of Conduct, the publisher also undertakes to maintain a responsible advertising policy, provide opportunities for consumer redress, maintain community standards and adhere to stringent standards for a safe online gaming environment. These include the need to maintain an effective and coherent privacy policy which must encompass the responsible collection, distribution, correction, and security of the personal details of users who must be given the opportunity to comment on any perceived misuse of their personal details and therefore be fully advised as to ways, for example, of avoiding unsolicited or unwanted e-mail contact.

Additionally, in 2013, the industry established IARC, The International Age Rating Coalition, which comprises rating boards from Europe, North America, Brazil and Australia who have joined forces to provide a solution for the globalised market of apps collectively representing regions serving approximately 1.5 billion people. IARC has now been adopted by Google Play Store, Microsoft Windows Store, Nintendo® eShop and the Sony PlayStation® Store and informs the consumer about certain types of functionality in an app, such as in-app purchases, location data sharing, unrestricted internet access and the ability of users to interact.

The PEGI system, in addition with the safety by design features adopted for U2U video games, aims to prevent harm to all users. Our members systems are deliberately designed to minimise sharing of and exposure to harmful content, with some platforms carefully restricting user-to-user contact through the sharing of friend codes and limiting groups to small numbers. This is particularly true of games designed for younger audiences, where social interaction is typically carefully controlled to the extent it is allowed at all.

The safety by design aspect also includes carrying impact assessments, done at the design stage to identify and reduce risks. it predates the 15 standards set out in the ICO's Age-Appropriate Design Code but reflects similar thinking. Additionally, through methods like age verification, manual interventions into account reclassification and survey-based research, companies can assess factors including on how people access their service, the number of child accounts created, as well as examine reported items of content as a proportion of overall content shared between users.

The industry provides various self-assessments on the state of its online chat rooms, analysing and moderating the contents, as well as to act if any harmful content is picked up. It mitigates risk of

disruptive content through their tools, including escalation policies for potentially unlawful activity or threats. The most common form of inappropriate content found in games is disruptive behaviour, such as toxic language or names, as opposed to unlawful behaviour or threats of harm. The industry is committed to tackling such disruptive behaviour, as it reduces the quality of the experience for other users and hence the appeal of the games themselves.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Enhanced user control (U2U)

Question 37:
i) Do you agree with our proposals?
Response: NA
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 38:
i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: NA
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 39:
i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response: NA
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

User access to services (U2U)

Question 40:
i) Do you agree with our proposals?
Response: Yes, we would agree that services should block the accounts of users that share CSAM. It is worth adding that in such rare yet severe circumstances, a report will also typically be made to relevant law enforcement authorities. As mentioned throughout this consultation response, many video game developers have in place collaboration with local law enforcement.
ii) Please provide the underlying arguments and evidence that support your views.
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:
i) What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response: Below we lay out examples of members practices to block users: A members internal practice is as follows: a user's username as well as their email address is banned, so it cannot be used again in future by another user. They *can* ban a user's IP address at the account level, and it will impact when the users tries to register a new account with any of the developers game. It is also possible for them to ban at the device level – so a single console can be banned from accessing any of the developers' online services. Additionally, a platform member said that they do not only permanently suspend the offender's account, but they also permanently prevent the offender's console connected to the uploading of CSAM from connecting to their network, placing a financial barrier between the offender and their ability to rejoin the consoles network. They have found device suspension to be an effective way to prohibit offenders from returning to the network. The device suspension also means users can not re-use the same email address across multiple accounts. However, both members found that blocking IP addresses is generally ineffective and can have the unintended consequence of punishing innocent players.

ii) What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response: NA
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 42:
i) How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response: Members impose permanent bans for any account holder sharing any CSAM, with zero exceptions. They do not see any reason to do otherwise. In such rare yet severe circumstances, a report will also typically be made to relevant law enforcement authorities.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:
i) What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response: It is practice of most members that any content that is classed as CSAM by an automated tool will have already been rejected from upload and the user who tried to upload will just be told to try another image. All suspected CSAM content caught by the automated tool is sent for human review. If the human reviewer decides it is not CSAM, the user will not be sanctioned. If the content is CSAM, the user will be banned and reported to law enforcement. Therefore, human review significantly mitigates the risk of impacting a user's rights.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response: No. See Answer to Question 15. Additionally, it would be good to get further guidance on what conditions companies can meet to move into the low-risk category.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response: No. See Answer to Question 15.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: As stated in response to earlier questions, the focus should be on the functionality of a service and the nature of communication and content-sharing it enables, and therefore on the overall risk profile for users, more than on raw numbers of people on a service.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response: NA	
ii)	What are the underlying arguments and evidence that inform your view?
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: No, it is 390 pages long and covers legal definitions of offences, requiring a determination of action, intent and defences which is beyond human moderator teams unless they are staffed by criminal lawyers. Many of our members simply don't have the financial capability of employing lawyers to scrutinise the detailed guidance. Ofcom rightly acknowledges these challenges and recognises that companies can focus on identifying content which is against the terms of use of a service, invariably capturing illegal content as well. This should be made simpler and clearer, for the benefit of companies of all sizes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: NA	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response: NA	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response: NA	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response: NA	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	