Consultation response form

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

Consultation title	Consultation: Protecting children from harms online
Organisation name	Ukie

Your response

Question	Your response
Volume 2: Identifying the services children are using Children's Access Assessments (Section 4).	
Do you agree with our proposals in relation to children's access assessments, in particular the aspects below. Please provide evidence to support your view. 1. Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance? 2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the factors that service providers consider in assessing whether the child user condition is met? 3. Our proposed approach to the process for children's access assessments?	Confidential – N *Q.1: Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance?* 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. 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. The overwhelming majority of companies have clear terms of service and act to remove any content or

Question	Your response
	interaction which breaches those terms, including any harmful content. Child and user safety is built into the companies' decision-making structures by default and by design. It is a core design principle. All services and software operate within that system and are subject to the same controls. 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. Additionally, members have long employed age assurance methods that we believe are "accurate, robust, reliable and fair" by verifying the age of the parent or guardian setting up the account through methods like mobile number verification, credit card checks, facial recognition, and photo-ID verification. 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. Additionally, the nature of online interaction within games is nuanced and specific and must be considered when setting guidance. 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. It is important to mention that the interactive entertainment industry varies greatly from other online platforms, including social media. Content is designed to meet our well-established age-appropriate standards, and where interactions between users are possible, they will typically

Question	Your response
	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. Additionally, the industry collects and stores game play data in a way that does not allow companies to identify the player directly by applying technical and organisational measures to prevent easy linking between the game play dataset and the players' platform account information. The industry has also since long endorsed the use of pseudonymised data as a valid way to protect identity of underage users. Specifically, the communication capabilities in games are usually far more restricted than the capabilities in social media platforms. It is almost always 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. We therefore agree with your proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance. However, we would like you to also consider, as you stated in the consultation specific webinars, that the measures that apply should depend on the 1) size of the service's UK user base, the 2) purpose of the service, and 3) other relevant characteristics and or functionalists. The second and third points should demonstrate the different nature of video games and other online services like social media. The third should also be taken into account by Ofcom when considering characteristics of measurements which constitute highly effective age assurance.

Question	Your response
	Any future changes to the criteria of 'highly effective age assurance' should be communicated clearly and consulted upon with the relevant parties. Separately, our members are requesting greater clarity on the scenarios in which age assurance is not required, particularly in relation to the statutory exception outlined in section 12(5) of the OSA. As referred to by the Online Safety team at Ofcom during the topical webinars, as well as the roundtable with Ukie's members, the age verification or age estimation requirement applies to providers for PPC harmful to children, except when (a) a term of service clearly prohibits such harmful content, and (b) this policy is enforced for all users. Obtaining further guidance from Ofcom on how the sector should interpret this exception would be beneficial not only for the sector but for all online services in terms of compliance. This is especially relevant for companies that explicitly prohibit PPC and PC in their terms and actively moderate content to remove such material for all users.
	Q.2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the fac-tors that service providers consider in assessing whether the child user condition is met? The current broad guidance will effectively mean that the vast majority of games companies will be included within the regulatory scope. This broad inclusion will have significant implications for the video games indus-try. Our members are worried that the guidance has been developed more with social media platforms in mind rather than games companies. Therefore, it is cru-cial to provide further clarity on what constitutes a "sig-nificant number of users who are children" and to under-stand the specific factors service providers should con-sider in assessing whether the child user condition is met. Additionally, our members would recommend some worked examples for the carious industries. Clear

Question	Your response
	definitions, examples and criteria will enable companies to accurately assess their compliance obligations. In Volume 1, Section 2.14, there is no definition of "significant number of users." We recommend requesting precise definitions for both "significant number" and "users." Without clear definitions, companies may struggle to determine their responsibilities, leading to potential over-compliance or under-compliance. A detailed understanding of these terms is essential for implementing appropriate measures and ensuring regulatory adherence. If this is not possible, our members urge Ofcom to work closely with the industry to develop specific guidance and worked examples. Furthermore, it is essential to differentiate between games companies and social media services. Unlike most social media platforms, which generally do not target specific age demographics, many games are designed for particular age groups. This distinction is significant because games often have built-in mechanisms for delivering age-appropriate content, unlike the broader, more general audience of social media platforms. Recognising this difference can help tailor the regulatory approach to suit the unique characteristics of the gaming industry. As we expand throughout this response, the games industry has many safeguards in place to support parents in the decision-making process of buying a game or adjusting parental tools, such as the Pan-European Game Information (PEGI) system, which aims to protect minors and behave responsibly where children are concerned Moreover, the calculation of user numbers in the video games industry needs special consideration. The method for determining user numbers should account for the unique user engagement patterns in games, which differ from those in social media. For instance, many games use age ratings and parental controls (such as PEGI) as forms of age assurance which operate 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. These

Question	Your response
	measures may not be as prevalent or effective in other types of online services. Understanding these nuances will help create a more accurate and fair regulatory framework for the video games industry. We raised the issue of user metrics and definition of users in previous consultations. It is worth noting also that video games, as a diverse and evolving medium, do not prioritise, promote, or profile content in the same way social media might. Adding to the previous point on defining a user, we acknowledge the importance of tracking monthly active users (MAU) as a key metric for regulatory compliance. However, it is crucial to consider that the calculation of MAU can vary significantly based on the criteria used for measurement. Therefore, we emphasise the need for a consistent definition of 'users' to ensure that MAU calculations remain accurate and comparable across different platforms and services. The lack of a standardised definition could result in confusion and misinterpretation of user metrics, potentially affecting regulatory compliance. Additionally, we believe the current definition of users in the Act does not consider the unique nature of video games, especially concerning the inclusion of 'passive' or 'unregistered' users. While it is essential to protect individuals who may be indirectly exposed to online harms, it is equally vital to avoid overinflating user numbers with dormant individuals who do not actively engage with a platform and their online functionalities. For instance, counting individuals who merely visit a game's home screen or download a game without any substantial interaction may not align with the primary objectives of the Act. Therefore, we recommend a thoughtful and nuanced approach to defining 'users' that takes into account the level of meaningful engagement required to warrant inclusion. Lastly, the games industry faces unique challenges in accurately tracking user numbers, particularly for free-to-play games where not all players create accounts. Distinguishing between repeat users and distinct individuals

Question	Your response
	becomes complex without accurate tracking mechanisms. An oversimplified tracking approach could result in misleadingly high user counts, which may not accurately represent the level of user engagement or the potential risks associated with a platform. Therefore, we encourage allowing for development of flexible tracking methods that can adapt to the diverse nature of online gaming, accounting for variations in user behaviour and account creation. *Q.3. Our proposed approach to the pro-cess for children's access assessments?* We understand the importance of assessing the risk of potential online harms for children, 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. This burden can have an overall disproportionate and negative effect on the video games industry as it curtails the innovation and diversity of the market by pushing the smaller developers out due to their inability to digest the complex requirements Ofcom sets for them. Our members therefore call on Ofcom to make proportionality the central focus when developing the guidance and risk assessments, 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 about the burden of the task, not just for the SMEs, but also for the larger services in the games sector.

Question	Your 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 harmful content that could potentially be shared. Any service that allows the sending of text could potentially be used to send almost any harmful 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 harmful 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 harmful 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 harmful content to be spread, without simultaneously

Question	Your response
	considering the mitigation measures that may have been adopted by the service provider, is disproportionate and makes the assessment process redundant. 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 unreasonable 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. Therefore, our members believe that mitigation measures should be taken into account when assessing the risk level. We also urge Ofcom to engage with members on this matter and provide clarification as priority. 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

Question	Your response
	are not Large Services for the purposes of Ofcom's guidance.
Volume 3: The causes and impacts of online harm to children **Draft Children's Register of Risk (Section 7)**	
Proposed approach: 4. Do you have any views on Ofcom's assessment of the causes and impacts of online harms? Please provide evidence to support your answer. a. Do you think we have missed anything important in our analysis? 5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer. 6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer. 7. Do you have any views on our interpretation of non-designated content or our approach to identifying non-designated content? Please provide evidence to support your answer. **Evidence gathering for future work:** 8. Do you have any evidence relating to kinds of content that increase the risk of harm from Primary Priority, Priority or Non-designated Content, when viewed in combination (to be considered as part of cumulative harm)?	Confidential? – N *Q.4 - Do you have any views on Ofcom's assessment of the causes and impacts of online harms? Please provide evidence to support your answer.* We are worried that Ofcom has not responded to us in regard to the concerns raised in Ukie's submission to your "Protecting people from illegal harms online" consultation (henceforth referenced as the Illegal Harms consultation). The consultation document shows 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) of the Illegal Harms consultation, 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

Question	Your response
9. Have you identified risks to children from GenAI content or applications on U2U or Search services? a) Please Provide any information about any risks identified 10. Do you have any specific evidence relevant to our assessment of body image content and depressive content as kinds of non-designated content? Specifically, we are interested in: a) (i) specific examples of body image or depressive content linked to significant harms to children, b. (ii) evidence distinguishing body image or depressive content from existing categories of priority or primary priority content. 11. Do you propose any other category of content that could meet the definition of NDC under the Act at this stage? Please provide evidence to support your answer.	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 sets 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 Ask About Games campaign. 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.

Question	Your response
	Underlying all of this work is the very nature of interaction and communication within games, which differs greatly from other online platforms, including social media. 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. Unlike social media, the purpose of the communication is to enable, enhance or complement the gameplay. The possibility to share harmful content is often very restricted merely by the design of the service. The comments in the consultation documents, and the assimilation with social media, indicate that Ofcom has not yet taken these fundamental differences into account. As part of this work, we would like to invite Ofcom representatives to visit a video game developer that creates online games accessed by children, so that Ofcom can get a first hand experience on the safety by design measures, and gain a better understanding of the unique nature of video games. --- *Q. 5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer.* Regarding Ofcom's interpretation of the links between risk factors and different kinds of content harmful to children, we believe that a more nuanced view is needed, particularly in the context of gaming services. Specifically, Section 7.4.65 of Volume 3 highlights that children on gaming platforms are at risk of encountering abuse and hate, especially through messaging functionalities. While this is a valid concern, and something members are acutely aware of and are tackling, it is essential to consider the proportionality of these issues within the gaming space compared to social media platforms.

Question	Your response
	On a related point, the available evidence base, and our members' combined experiences, make clear that our industry sees significantly lower rates of harmful content sharing than many other online services. As mentioned in the previous questions, a study found 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. The games industry is a leader in keeping players safe online. Additionally, many video games services incorporate comprehensive moderation systems and real-time monitoring to detect and address inappropriate behaviour promptly. Unlike social media platforms, where user interactions are more open-ended and less controlled, gaming environments typically restrict user-to-user contact through mechanisms like friend codes and limit group sizes, especially in games designed for younger audiences. This controlled environment significantly reduces the risk of children encountering harmful content. Furthermore, our members have embedded child and user safety into their decision-making structures by default and by design. This commitment to safety is not an afterthought but a core design principle. All services and software in the gaming sector operate within a system that emphasises safety and privacy from the outset. For example, when children first access a new platform, such as a console or an online store, they are required to self-declare their age, and are often required to be accompanied by a parent. This initial step ensures that age-appropriate content and interactions are provided from the beginning. The industry has long adopted Privacy by Design as a key principle, even before the enforcement of GDPR. Gameplay data is typically collected and stored in ways that prevent the direct identification of players. Technical and organisational measures are applied to ensure that gameplay datasets cannot be easily linked to the players' platform account information. Pseudonymised data is

Question	Your response
	used to protect the identity of underaged users, adhering to GDPR requirements that limit the collection and visibility of personal data. Moreover, video game companies often employ technical and organisational measures to prevent linking gameplay data with identifiable information. Such anonymised or pseudonymised datasets allow for personalised user experiences while maintaining a high level of privacy and safety. This approach contrasts with social media platforms, where personal data is often more readily accessible and potentially exploitable. We are encouraged by the 16 standards of age-appropriate design proposed in the ICO Code, which effectively recognise the proactive measures we have been implementing. Ofcom's recent research supports our approach, noting that many parents consider their child's maturity and the perceived risk of the platform when deciding on accessibility. Concerns about data sharing for age assurance and a preference for guardian confirmation as a method of age assurance also align with the industry's practices, which aim to empower parents in managing their children's online activities. The most common form of inappropriate content found in games is disruptive behaviour, such as toxic language or inappropriate usernames, rather than 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. However, such work largely falls outside Ofcom's remit. To support parents in the decision-making process of buying a game or adjusting parental tools, the industry has committed to adopting the PEGI system to protect minors and behave responsibly where children are concerned. Each publisher that joins PEGI must sign a Code of Conduct, committing to providing parents with objective, intelligible, and reliable information regarding the

Question	Your response
	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. Additionally, the industry established the International Age Rating Coalition (IARC) in 2013, comprising rating boards from Europe, North America, Brazil, and Australia. IARC provides a solution for the globalised market of apps, informing consumers about functionalities such as in-app purchases, location data sharing, unrestricted internet access, and user interaction capabilities. This coalition ensures consistent age rating standards across major platforms like Google Play Store, Microsoft Windows Store, Nintendo® eShop, and Sony PlayStation® Store. On a separate note, we also wanted to highlight that video games have a more positive impact on brain development in children compared to video games. A recent study from found that “children who devote more time to playing video games had a weak increase in cerebellum volume during the critical developmental window of development… while those who spent more time using social media had a subtle decrease in cerebellum volume.” Our members reiterate the opportunity for them to demonstrate to Ofcom their safety by design measures during a visit to a developer’s studio.
Draft Guidance on Content Harmful to Children (Section 8)	

Question	Your response
12. Do you agree with our proposed approach, including the level of specificity of examples given and the proposal to include contextual information for services to consider? 13. Do you have further evidence that can support the guidance provided on different kinds of content harmful to children? 14. For each of the harms discussed, are there additional categories of content that Ofcom a) should consider to be harmful or b) consider not to be harmful or c) where our current proposals should be reconsidered?	Confidential? – Y / N
Volume 4: How should services assess the risk of online harms? **Governance and Accountability (Section 11)**	
15. Do you agree with the proposed governance measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 16. Do you agree with our assumption that the proposed governance measures for Children's Safety Codes could be implemented through the same process as the equivalent draft Illegal Content Codes?	Confidential? – Y / N

Question	Your response
Children's Risk Assessment Guidance and Children's Risk Profiles' (Section 12)	
17. What do you think about our proposals in relation to the Children's Risk Assessment Guidance? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. 18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. Specifically, we welcome evidence from regulated services on the following: 19. Do you think the four-step risk assessment process and the Children's Risk Profiles are useful models to help services understand the risks that their services pose to children and comply with their child risk assessment obligations under the Act? 20. Are there any specific aspects of the children's risk assessment duties that you consider need additional guidance beyond what we have proposed in our draft? 21. Are the Children's Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service? a) If you have comments or input related to the links between different kinds of content harmful to children and risk factors, please refer to Volume 3: Causes and Impacts of Harms	Confidential? – N *Q. 17. What do you think about our proposals in relation to the Children's Risk Assessment Guidance?* 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 harmful content that could potentially be shared. Any service that allows the sending of text could potentially be used to send almost any harmful 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 harmful content to appear on their services in determining whether their services are low risk, multi-risk or high-risk. Past experience of run-

Question	Your response
to Children Online which includes the draft Children's Register of Risks.	ning that service, or similar services, should be an important factor in this. 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 harmful 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. As mentioned to our response to Q.3, our members request any mitigations measures should be considered prior to the assignment of the risk rating. The goal of the risk assessment process should be to assess the actual risk of harmful content appearing on the service in question, not the risk of harmful 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

Question	Your response
	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 a lead of logic to conclude that a service is 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 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

Question	Your response
	UGC. If there are UGC, we recommend that Ofcom analyses the service and it's functionalities features, as well as the moderation and community standards. 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 harmful content, if any, that is shared on that or similar services they have run. --- *Q. 18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children?* See previous answer. Additionally, 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. This is something we highlighted in previous consultation responses, namely the Illegal Harms consultation. 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

Question	Your response
	is readily available to provide more evidence on this matter. --- *Q. 19. Do you think the four-step risk assessment process and the Children's Risk Profiles are useful models to help services understand the risks that their services pose to children and comply with their child risk assessment obligations under the Act?* As mentioned in our submission to the Illegal Harms consultation, we believe that the threshold for carrying out a new risk assessment is unworkable. Additionally, as mentioned in our response to Q.3, the low threshold risks disproportionally affecting the smaller companies, risking curtailing the innovation and diversity of the market by pushing the smaller developers out due to their inability to digest the complex requirements Ofcom sets for them. 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 unfeasible – 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.

Question	Your response
	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.
	Q.20 Are there any specific aspects of the children's risk assessment duties that you consider need additional guidance beyond what we have proposed in our draft? We appreciate the comprehensive framework laid out in the draft Children's Risk Assessment Guidance, yet there are specific aspects where additional clarity and guidance would be beneficial. Firstly, the assessment of risk must consider the nature of the service, specifically the types of communication allowed and the mitigation measures adopted by the service provider. The potential for harmful content varies significantly depending on these factors. For instance, text-based communication can potentially transmit almost any harmful content, whereas the scope of content in voice or video formats is different. This nuance must be accounted for in the guidance. Gaming services typically feature more restricted communication capabilities compared to social media platforms. Communication in games is often ancillary to the primary purpose of gameplay, intended to enhance or support the game rather than facilitate open-ended discussions. Consequently, the potential for harmful content transmission is considerably lower. The guidance should explicitly allow game providers to assess the feasibility of harmful activity on their platforms, factoring in past experiences and existing mitigation measures. The proposed measures state that services should assess the risks of harm that children might face by using the risk factors identified in the draft Children's Risk Profiles and evaluate the likelihood and impact of harmful content. This involves considering the characteristics of the service that might increase or decrease risks of harm, such as how the service is used, its features, and the risk

Question	Your response
	of cumulative harm. While this approach is sound, it is crucial to emphasise that the actual risk of harmful content should be assessed, considering the mitigation measures in place. Evaluating the service absent these measures leads to an inaccurate risk profile. The guidance should encourage companies to use risk assessments to identify areas requiring more attention and adjust their risk evaluations based on the effectiveness of their implemented safeguards. When determining the risk level of identified harms, it is crucial to consider the frequency and context of these occurrences. For example, an isolated incident should not automatically elevate a service to a medium or high-risk category. The guidance should allow for a more holistic evaluation, considering factors such as the proportion of total complaints related to the harm and the effectiveness of measures to prevent such incidents. A singular occurrence should not disproportionately impact the risk designation of a service. Given the complexity of the gaming industry, especially for start-ups, micro, and SMEs, the burden of conducting individual risk assessments for each service can be overwhelming. It would be proportionate to allow service providers to use a single risk assessment for multiple services with similar functionalities and mitigation measures, especially when these services are not classified as large under Ofcom's guidelines. Additionally, the obligations outlined in the guidance seem to adopt a one-size-fits-all approach, not adequately distinguishing between social media platforms and online games with user-generated content (UGC). The Australian Online Safety Act and the EU's Digital Services Act set differing compliance requirements based on the types of services and associated risks. Similarly, the guidance should differentiate U2U services by their primary functionality and the nature of UGC shared. If there is no sharing of UGC, the obligations should be less stringent, reflecting the lower overall risk.

Question	Your response
	Q. 21. Are the Children's Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service? The clarity and proportionality of the Children's Risk Profiles are crucial to effectively understanding and managing the risks associated with content harmful to children on our services. The current guidance provides a structured approach to identifying and assessing these risks, which is beneficial. However, some enhancements could improve its effectiveness. Firstly, the step-by-step process outlined for consulting the Children's U2U Risk Profile is clear and methodical. Answering the 'Yes' or 'No' questions to identify specific risk factors relevant to our services is a straightforward method. The inclusion of a glossary to help interpret these risk factors further aids in understanding and applying the guidance. This clarity is essential for ensuring that all service providers, regardless of their size or resources, can effectively use the risk profile. However, while the structured approach is helpful, the proportionality of the guidance could be improved. The guidance should more explicitly differentiate between the varying natures of different services, particularly distinguishing between platforms like social media and online games. The communication capabilities in games are typically far more restricted and ancillary to the core gameplay features. This means that the potential for harmful content transmission is considerably lower compared to social media platforms, where open forums and long-term conversations are more common. It is also important to emphasise that the risk assessment should focus on the actual risks presented by the service, considering the mitigation measures already in place. Many video games services, for example, report exceedingly rare instances of harmful content due to their robust safeguards. Suggesting that these services

Question	Your response
	are automatically medium or high risk without considering their specific context and mitigation efforts is disproportionate. The guidance should allow for a more nuanced assessment that takes into account the nature of user interactions, the functionalities available, and past experiences with harmful content. Additionally, the guidance should provide more detailed instructions on how to integrate the identified risk factors into the overall risk assessment process. While the steps to select relevant risk factors are clear, the subsequent process of assessing how these factors affect the service and determining appropriate mitigations could benefit from further elaboration. This would help ensure that the risk assessment is not only comprehensive but also practical and tailored to the specific characteristics of each service.
Volume 5 – What should services do to mitigate the risk of online harms **Our proposals for the Children's Safety Codes (Section 13)**	
Proposed measures 22. Do you agree with our proposed package of measures for the first Children's Safety Codes? a) If not, please explain why. **Evidence gathering for future work.** 23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration? a) If so, please provide evidence of the impact, effectiveness and cost of such measures, including any results from trialling or testing of measures. 24. Are there other areas in which we should consider potential future measures for the Children's Safety Codes?	Confidential? – N *Q. 22. Do you agree with our proposed package of measures for the first Children's Safety Codes?* Ukie's members agree with Ofcom's proposed safety measures to mitigate the risks to children. The video games industry has consistently demonstrated a proactive approach in implementing robust safety measures that align closely with proposed Children's Safety Codes. For instance, major games platforms have integrated comprehensive parental controls and age verification systems. These tools empower parents to manage their children's gaming experiences effectively. Parents can set limits on screen time, restrict access to age-inappropriate content, and control online interactions, ensuring that young users can only access content that is suitable for their age group. These measures not only enhance parental oversight but also contribute significantly to the overall safety and well-being of young players on gaming platforms.

Question	Your response
a) If so, please explain why and provide supporting evidence.	In terms of content moderation, gaming companies have implemented both automated systems and human moderators to oversee player interactions. Automated systems scan in-game chats and interactions in real-time to detect inappropriate behaviour or content. Human moderators complement these systems by reviewing reported cases and taking swift action against violations of community guidelines. Players are also provided with robust reporting tools that allow them to flag concerns directly, which are then promptly investigated and addressed by moderation teams. This proactive approach to moderation helps foster a respectful and safe community atmosphere within online gaming environments. Additionally, governance structures within gaming companies emphasise accountability and compliance with safety standards. Companies appoint specific individuals responsible for child safety and conduct regular reviews of their practices to ensure ongoing adherence to safety guidelines. These individuals oversee the implementation of age verification measures, content moderation policies, and the effectiveness of parental control tools. By maintaining clear lines of accountability and regularly updating protocols to address emerging risks, gaming companies demonstrate their commitment to upholding high standards of safety across their platforms. Furthermore, gaming companies provide educational resources and support tools to empower parents and children to navigate online environments safely. These resources include detailed information on how to use parental controls effectively, guidelines on online safety, and instructions on how to report harmful content or behaviour. By equipping users with these resources, gaming companies aim to educate and empower families to make informed decisions about online gaming and ensure a positive and safe experience for all players, particularly children. Lastly, the industry's commitment to safety extends globally, with gaming companies ensuring compliance

Question	Your response
	with international standards and regulations on child safety. This includes implementing age verification measures and content moderation practices that meet the diverse regulatory expectations across different regions. By adhering to these standards and collaborating with regulatory bodies, gaming companies fulfill their responsibility to provide safe and age-appropriate digital experiences for children worldwide. *Q. 23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration?* The video games industry's commitment to ensuring child safety online extends beyond mere compliance with regulatory frameworks; it involves proactive measures embedded in the design, development, and operation of gaming platforms and services. One of the fundamental approaches embraced by industry leaders is the concept of "safety by design." This principle emphasises integrating safety considerations into every stage of the game development process, from initial concept through to release and ongoing updates. The ways these are implemented vary per game. Detection mechanisms play a crucial role in identifying and addressing potential risks in real-time. Advanced AI and machine learning technologies are increasingly deployed to scan and analyse in-game interactions, chat logs, and user-generated content for signs of toxicity, inappropriate behaviour, or harmful content. This proactive monitoring helps swiftly identify and address issues before they escalate, thereby promoting a safer gaming experience for children and other users alike. Moreover, intervention strategies are pivotal in responding promptly to incidents and providing support to affected players. Many game platforms offer tools that empower players to block, mute, or report abusive behaviour or content, thereby giving individuals greater control over their online interactions. Additionally, dedicated support teams and customer service channels are

Question	Your response
	available to handle reports of harmful behaviour, ensuring that concerns are addressed swiftly and effectively. In addition to proactive safety measures, many game developers implement innovative features like reputation systems and communication tools such as the ping system to further enhance player safety and engagement. Reputation systems track player behaviour and interactions within the game environment, assigning ratings or scores based on factors like sportsmanship, helpfulness, and adherence to community guidelines. This encourages positive conduct among players and discourages toxic behaviours by highlighting and rewarding good behaviour while applying penalties for misconduct. Similarly, communication tools like the ping system allow players to convey strategic information without the need for verbal communication, reducing the potential for misunderstandings or conflicts that could escalate into harmful interactions. These tools are designed not only to improve gameplay coordination but also to promote a collaborative and respectful gaming atmosphere where players can effectively communicate without resorting to negative or abusive language. By integrating these incentive-based systems into their games, developers not only prioritise gameplay experience but also actively contribute to fostering a safer and more inclusive gaming environment. These features encourage responsible and respectful behaviour among players while empowering individuals to actively contribute to maintaining a positive community atmosphere. As such, these innovative tools complement broader safety measures, reinforcing the industry's commitment to promoting a secure and enjoyable gaming experience for players of all ages. Beyond technical solutions, industry initiatives also include educational campaigns and resources aimed at promoting digital literacy and responsible online behaviour among players and parents. These efforts range

Question	Your response
	from online safety guides and tutorials integrated into gaming platforms to partnerships with educators and advocacy groups to deliver targeted educational content on topics like cyberbullying, privacy protection, and safe online gaming practices. In essence, the video games industry's multifaceted approach to child safety online reflects its commitment to fostering a positive and secure gaming environment. By combining innovative technologies with proactive community management and educational outreach, game developers and publishers continue to evolve their strategies to meet the challenges of an ever-changing digital landscape while prioritising the well-being of young players. In addition to the safety aspects, we believe that the interactive nature of games fosters critical thinking and problem-solving skills. Many games require players to evaluate information, make decisions, and solve complex problems, which translates to improved critical evaluation of media content. Additionally, games that simulate real-world scenarios or allow players to role-play help users understand complex issues such as the impact of misinformation and the consequences of online actions, making abstract concepts more concrete and relatable. Evidence to suggest this can be found in the Power of Play report[1], published by Ukie and other global video games association in September 2023, which surveyed 13,000 players (aged 16 and older) and found that players believing that it has improved their: • Creativity: 75% in the UK, 73% globally; 73% in Europe; • Problem-solving skills: 87% in the UK, 69% globally; 66% in Europe; • Cognitive Skills: 73% in the UK, 69% globally, 68% in Europe, • Teamwork and collaboration skills: 73% in the UK, 69% globally, 68% Europe,

[1] https://ukie.org.uk/download/46zpjdq8j4ezz7gevd4kp5p4cp/0

Question	Your response
	Furthermore, social interaction and collaboration in multiplayer games and online gaming communities expose players to diverse viewpoints and teach them to navigate digital interactions responsibly. This exposure is crucial for recognising and countering misinformation. Moreover, games with strong moderation and community guidelines model appropriate online behaviour and highlight the importance of respectful digital interaction, promoting digital citizenship. These teachings that are gathered through the moderation process are often shared with 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.

Developing the Children's Safety Codes: Our framework (Section 14)	
25. Do you agree with our approach to developing the proposed measures for the Children's Safety Codes? a) If not, please explain why. 26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in how systems and processes manage both content harmful to children and illegal content? a) Please explain your views. 27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children? 28. Do you agree with our definition of 'large' and with how we apply this in our recommendations? 29. Do you agree with our definition of 'multi-risk' and with how we apply this in our recommendations? 30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk?	Confidential? – N *Q. 25. Do you agree with our approach to developing the proposed measures for the Children Safety Codes?* 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 harmful 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. Therefore, our members believe that the broadness of some of the guidance risks undoing the long record of safety measures which are already in place, and we thus encourage Ofcom to include the mitigation measures already in place when assessing the risk level. The nature of online interaction within games is nuanced and specific and must be considered when considering children safety online. 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. *Q. 26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in*

	how systems and processes manage both content harmful to children and illegal content? See answer above. --- *Q. 27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children?* 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. We would like to draw the attention to our response to Q.29, which explains in detail the importance of proportionality. --- *Q. 28. Do you agree with our definition of 'large' and with how we apply this in our recommendations?* 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? 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 and/or harmful 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. --- *Q.29. Do you agree with our definition of 'multi-risk' and with how we apply this in our recommendations?* 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. 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.
	Q. 30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk? 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 harmful 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 harmful 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 harmful 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 harmful 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 harmful 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 harmful 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 harmful 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. On the latter, our members urge Ofcom to engage with the industry to understand an important distinction to other online services, namely that game developers and publishers often release multiple game titles in a calendar year. This frequency is something not relevant to social media companies.

Age assurance measures (Section 15)	
31. Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6? Please provide any information or evidence to support your views. a) Are there any cases in which HEAA may not be appropriate and proportionate? b) In this case, are there alternative approaches to age assurance which would be better suited? 32. Do you agree with the scope of the services captured by AA1-6? 33. Do you have any information or evidence on different ways that services could use highly effective age assurance to meet the outcome that children are prevented from encountering identified PPC, or protected from encountering identified PC under Measures AA3 and AA4, respectively? 34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services? a) Please provide any supporting information or evidence in support of your views. 35. Do you have any information or evidence on other ways that services could consider different age groups when using age assurance to protect children in age groups judged to be at risk of harm from encountering PC?	Confidential? – N We appreciate the proposal to recommend the use of highly effective age assurance (HEAA) to support Measures AA1-6. Given the shift from self-declaration of age to more robust age assurance measures, it is crucial to consider the effectiveness and appropriateness of these measures within different contexts. This transition from self-declaration to more robust age verification measures represents a critical step forward in enhancing child safety in digital environments. The gaming industry, in particular, has been proactive in implementing stringent age verification protocols as part of its broader commitment to safety by design. Measures such as age gates at the point of entry ensure that age-appropriate content and interactions are provided from the outset, minimising the risk of children accessing inappropriate material. Furthermore, the adoption of Privacy by Design principles ensures that gameplay data is handled responsibly, protecting the identity of underage users and complying with privacy regulations like GDPR. While HEAA is generally effective, there are contexts where its applicability may warrant further consideration. For instance, in environments where the dissemination of proprietary or non-user-generated content is predominant, such as in video games depicting publisher-created scenes, the necessity of Measure AA2 should be contingent upon the centrality of user-generated content (UGC) to the platform's purpose. Clarifying this criterion is essential to avoid imposing unnecessary or disproportionate age assurance requirements on platforms where UGC is not a primary feature. In cases where HEAA may not be suitable or proportionate, alternative approaches can complement or substitute stringent age verification methods. For example, enhancing parental control functionalities allows parents to manage and monitor their children's access to content based on age appropriateness. This empowers parents to make informed decisions about their children's online

	activities while respecting their role as primary caregivers. Moreover, employing contextual age assurance strategies that tailor verification methods based on the nature and interactivity of content can strike a balance between security and user experience. This approach ensures that more intrusive age verification measures are reserved for interactive features where the risk of exposure to inappropriate content is higher. It is crucial to maintain flexibility in age assurance requirements. This flexibility allows for nuanced application across different digital environments, considering factors such as the centrality of UGC and the availability of alternative safeguards like parental controls. By fostering a multi-layered approach to child safety online, incorporating both robust age verification and user-friendly controls, the gaming industry can continue to uphold high standards of protection while promoting a positive and secure digital experience for children and families alike.
Content moderation U2U (Section 16)	
36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 37. Do you agree with the proposed addition of Measure 4G to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – N *Q. 36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.* 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 Ask About Games 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 harmful, ssers 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 harmful 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 players 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.

	Separately, and as previously mentioned, proportionality of scale 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.
Search moderation (Section 17)	
38. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 39. Are there additional steps that services take to protect children from the harms set out in the Act? a) If so, how effective are they? 40. Regarding Measure SM2, do you agree that it is proportionate to preclude users believed to be a child from turning the safe search settings off? The use of Generative AI (GenAI), see Introduction to Volume 5, to facilitate search is an emerging development, which may include where search services have integrated GenAI into their functionalities, as well as where standalone GenAI services perform search functions. There is currently limited evidence on how the use of GenAI in search services may affect	Confidential? – Y / N NA

the implementation of the safety measures as set out in this code. We welcome further evidence from stakeholders on the following questions and please provider arguments and evidence to support your views: 41. Do you consider that it is technically feasible to apply the proposed code measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? 42. What additional search moderation measures might be applicable where GenAI performs or is integrated into search functions?	

User reporting and complaints (Section 18)	
43. Do you agree with the proposed user reporting measures to be included in the draft Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence.	Confidential? – N *Q. 43. Do you agree with the proposed user reporting measures to be included in the draft Children's Safety Codes?* We believe our response to Q.28 (i) and (ii) in our submission to the Illegal Harms consultation provides a relevant answer. We have copied it below for your convenience: 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

b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 45. Do you agree with the inclusion of the proposed changes to Measures UR2 and UR3 in the Illegal Content Codes (Measures 5B and 5C)? a) Please provide any arguments and supporting evidence.	latter method would empower the user with more relevant information. 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 harmful (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. *Q. 44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints?* Our members agree. *Q. 45. Do you agree with the inclusion of the proposed changes to Measures UR2 and UR3 in the Illegal Content Codes (Measures 5B and 5C)?* Our members agree.

Terms of service and publicly available statements (Section 19)	
46. Do you agree with the proposed Terms of Service / Publicly Available Statements measures to be included in the Children's Safety Codes? a) Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children? 48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – N *Q. 47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children?* On Terms of service, our members wish to highlight that, given the OSA's information 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 of making terms of service 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 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 service to a webpage containing the required info in the OSA would be a preferable way of meeting the OSA's information requirements. To further expand on this point, for many Ukie member companies, if an offense is confirmed then the in-game messages and emails sent to the player's account will clearly detail the actions taken, even if it is just a warning. They will also direct the player to the company's code of conduct and terms of service, emphasizing that repeated offenses will result in more severe penalties.

	The video games industry is committed to fostering positive and safe player communities, and various companies have implemented user support materials and functionalities to assist users in understanding and navigating terms of service and related products. For example, many industry leaders are active members of the Fair Play Alliance, a coalition of studios and publishers dedicated to reducing player toxicity and enhancing player safety. This collaboration allows companies to exchange ideas and develop effective solutions for managing player behaviour. Additionally, industry efforts include partnerships with organisations like Safe in Our World to create resources such as the Good Game Playbook, a dynamic tool for prevention and awareness of harmful behaviours.
Recommender systems (Section 20)	
49. Do you agree with the proposed recommender systems measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 50. Are there any intervention points in the design of recommender systems that we have not considered	Confidential? – N NA

here that could effectively prevent children from being recommended primary priority content and protect children from encountering priority and non-designated content? 51. Is there any evidence that suggests recommender systems are a risk factor associated with bullying? If so, please provide this in response to Measures RS2 and RS3 proposed in this chapter. 52. We plan to include in our RS2 and RS3, that services limit the prominence of content that we are proposing to be classified as non-designated content (NDC), namely depressive content and body image content. This is subject to our consultation on the classification of these content categories as NDC. Do you agree with this proposal? Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3. • Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3.	
User support (Section 21)	
53. Do you agree with the proposed user support measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our Illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.	Confidential? – N We wholeheartedly support the proposed user support measures outlined in the Children's Safety Codes. Our industry has a longstanding commitment to ensuring the safety and well-being of young users across online platforms. Through proactive measures and continuous innovation, video game companies have already integrated many of these safeguards into their services to protect children from potential harms. 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. For instance, providing children with the option to accept or decline invites to group chats (US1) is a feature that numerous video game platforms have already implemented. This empowers children to control their social interactions and minimizes exposure to inappropriate content within group settings. Similarly, the option to block and mute other users' accounts (US2) is widely employed across various gaming platforms, enabling users to mitigate instances of bullying, abuse, and other harmful behaviours effectively. Furthermore, the practice of allowing children to disable comments on their own posts (US3) is a standard feature in many video games with social components. This ensures that young users can manage their online presence and interactions in a manner that aligns with their personal safety preferences. Video game companies are committed to enhancing user control and privacy, and this measure exemplifies our industry's proactive approach in safeguarding children online. In addition to these measures, video game companies have invested in robust moderation systems to swiftly address content harmful to children (US2). These systems are designed to detect and remove inappropriate content, thereby maintaining a safer environment for young players. Furthermore, the provision of age-appropriate user support materials (US6) is a priority for the industry, as it ensures that educational resources and

	guidance are readily available to help children navigate online challenges responsibly. Overall, the video games industry is dedicated to advancing the safety and well-being of young users through proactive measures and continuous improvement of safety protocols. We view the proposed user support measures as complementary to our ongoing efforts and are committed to collaborating with regulatory bodies to implement effective safeguards that protect children while preserving the positive aspects of online gaming experiences. By working together, we can ensure that children can enjoy the benefits of interactive online platforms in a safe and supportive environment.
Search features, functionalities and user support (Section 22)	
54. Do you agree with our proposals? Please provide underlying arguments and evidence to support your views. 55. Do you have additional evidence relating to children's use of search services and the impact of search functionalities on children's behaviour? 56. Are there additional steps that you take to protect children from harms as set out in the Act? a) If so, how effective are they? As referenced in the Overview of Codes, Section 13 and Section 17, the use of GenAI to facilitate search is an emerging development and there is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this section. We welcome further evidence from stakeholders on the following questions and please provide arguments and evidence to support your views:	Confidential? – Y / N

57. Do you consider that it is technically feasible to apply the proposed codes measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? Please provide arguments and evidence to support your views.	

Combined Impact Assessment (Section 23)	
58. Do you agree that our package of proposed measures is proportionate, taking into account the impact on children's safety online as well as the implications on different kinds of services?	Confidential? – N The proposal for a package of measures aimed at enhancing children's safety online, while commendable in its intentions, may not be entirely proportionate when considering its potential impact across the diverse spectrum of services within the video games industry. Firstly, while the measures outlined in the Children's Safety Codes are comprehensive, they appear to adopt a somewhat uniform approach across different types of services. As argued throughout this consultation, this one-size-fits-all approach fails to adequately account for the distinct characteristics and functionalities of various platforms and games. For instance, smaller indie developers or start-ups may find it disproportionately burdensome to implement complex age verification systems or sophisticated content moderation tools, especially when their resources are limited compared to larger corporations. Moreover, the proposed measures emphasize stringent requirements such as robust age checks and comprehensive moderation systems. While these are essential for platforms with extensive user interactions or significant risks of harmful content, they might not be equally necessary or feasible for simpler games or niche applications where user interactions are limited and closely monitored. Imposing such stringent measures uniformly across all services could stifle innovation and impose unnecessary regulatory burdens, particularly on smaller entities that play a crucial role in driving creativity and diversity within the gaming industry. 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 hamrful 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. Additionally, the regulatory framework needs to be mindful of global considerations and differences in regulatory environments. Video game services operate on a global scale, adhering to various regional regulations and cultural norms. A rigid set of regulatory requirements may inadvertently conflict with existing frameworks in other jurisdictions or pose compliance challenges, especially for companies operating internationally. Furthermore, while the intent behind providing age-appropriate user support materials and crisis prevention information is laudable, the practical implementation and effectiveness of these measures across different platforms warrant careful consideration. Ensuring that these resources are accessible, comprehensible, and effective for children across diverse demographic and cultural backgrounds requires tailored approaches that acknowledge these variations.
Statutory tests (Section 24)	
59. Do you agree that our proposals, in particular our proposed recommendations for the draft Children's Safety Codes, are appropriate in the light of the matters to which we must have regard? a) If not, please explain why.	Confidential? – N While the intentions behind the proposed recommendations are commendable, particularly in aiming to enhance child safety in digital environments, several aspects warrant a critical examination. The recommendations, as currently structured, suggest a uniform approach that may not sufficiently account for the diverse nature of services within the video games sector. This sector encompasses a wide array of platforms ranging from simple games with minimal user interactions to complex multiplayer environments with extensive social features.

	The proposed measures, such as robust age verification systems and comprehensive moderation tools, are undeniably essential for platforms where users have extensive interactions and where there is a heightened risk of exposure to harmful content. However, applying these stringent requirements uniformly across all services could disproportionately burden smaller developers and start-ups. These entities often operate with limited resources and may struggle to implement such complex systems effectively, potentially stifling innovation and diversity within the industry. Moreover, the global nature of the video games market necessitates consideration of international regulatory variations and cultural differences. A rigid set of recommendations may inadvertently clash with existing regulatory frameworks in other jurisdictions or pose compliance challenges for companies operating internationally. This could lead to fragmentation and inconsistency in regulatory compliance efforts, complicating efforts to achieve a cohesive approach to child safety across borders. Furthermore, while providing age-appropriate user support materials and crisis prevention information is crucial, the effectiveness of these measures across diverse demographic and cultural backgrounds requires careful consideration. Ensuring that these resources are accessible and culturally relevant to children worldwide demands a nuanced approach that acknowledges and respects regional differences in digital literacy and online safety awareness. As mentioned throughout this response, we believe that Ofcom still lacks a clear understanding of the video games sector. To rectify this, our members have put themselves forward to invite Ofcom Online Safety representatives to visit their development studios to discuss the modus operandi of the game sector. The available evidence base, and our members' combined experiences, make clear that our industry sees significantly lower rates of harmful content sharing than many other

	online services. 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.
Annexes **Impact Assessments (Annex A14)**	
60. In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? 61. In relation to our Welsh language assessment, do you agree that our proposals are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English? a) 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.	Confidential? – Y / N

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