Consultation response form

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

Consultation title	Additional Safety Measures Consultation
Full name	Dominic Murphy
Contact phone number	(+44) 7834 098692
Representing (delete as appropriate)	Organisation
Organisation name	Ukie
Email address	dominic@ukie.org.uk

Confidentiality

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

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Whole response
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	Whole response
For confidential responses, can Ofcom publish a reference to the contents of your response?	Yes

Your response

Question	Your response
Question 1: Do you have further evidence regarding the harms and risks to users from livestreamed illegal content or content harmful to children, or harms and risks to children from broadcasting livestreams?	Ukie is the trade body for the UK's video games and interactive entertainment industry. A not-for-profit, it represents more than 700 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. The video games industry recognises the importance of proportionate and effective measures to mitigate potential risks arising from livestreamed content. However, it is essential to emphasise that the nature, function, and audience of livestreaming within video games environments are fundamentally different from livestreaming on social media platforms. As such, Ofcom's proposals under measures such as ICU D17, ICU C16, and ICU F3 risk applying inappropriate and disproportionate obligations to services that are demonstrably low risk. Before addressing livestreaming specifically, Ukie and its members wish to highlight a core concern that will recur throughout this response. Our members believe that Ofcom continues to expand and revise the regulatory framework before the existing codes of practice have been allowed to bed in and demonstrate their effectiveness. The Illegal Harms and Children's Safety Codes of Practice were finalised only recently, yet Ofcom is already consulting on a new set of requirements that go significantly beyond them. This approach creates a moving target for compliance and an unstable regulatory environment for companies that have already invested heavily in alignment. Repeated changes of this kind undermine confidence and increase cost without improving safety outcomes. Many Ukie members, including large publishers operating multiple user-to-user services, have already completed two full rounds of risk assessments and compliance updates as Ofcom's earlier draft and final codes evolved. To require a third revision now, while implementation of the existing

Question	Your response
	codes is still underway, would be disproportionate. The three-month implementation window currently proposed is particularly unrealistic given the technical, operational, and training demands these measures would create. Ukie therefore urges Ofcom not to introduce any new livestreaming obligations before summer next year at the earliest, and to guarantee a minimum implementation period of six to nine months once finalised. Turning to the livestreaming proposals themselves, Ukie's members do not believe that the available evidence supports the level of regulatory intervention currently proposed. Livestreaming within video games environments is typically structured, community-based, and embedded within a framework of long-standing safety-by-design practices. It differs materially from social media livestreaming, which tends to involve large, anonymous audiences and open-ended interaction. In games, livestreaming serves to enhance shared play experiences and collaboration, not to broadcast content to the public. Communication is generally limited in duration and reach, often restricted to friends, pre-approved followers, or in-game teams. In addition, most games platforms already include comprehensive safeguards that address the concerns Ofcom raises. Parental control systems on PlayStation Network, Xbox Live, and Nintendo Switch Online restrict livestreaming by default for child accounts and require parental permission to activate such features. These ecosystems also employ real-time moderation, word and image filters, and robust user reporting tools. Many publishers have introduced further safety mechanisms, including delay buffers that allow time for moderation before content is made visible and automated systems that flag high-risk behaviour or distress signals. These measures collectively meet the intended outcomes of ICU D17, ICU C16, and ICU F3 without the need for blanket human moderation or additional prescriptive obligations. Available evidence reinforces the view that the risk of harmful or illegal livestreamed content in video games is extremely low. Data from the National Centre for Missing and Exploited Children's CyberTipline report for 2022 shows that, out of more than thirty-two million global reports of child sexual abuse material, only eight thousand

Question	Your response
	two hundred originated from video game platforms, approximately 0.00025 per cent of the total. This demonstrates that the safety-by-design approach employed by the sector is both effective and proportionate. It is also important to note that livestreaming in games is subject to significant platform-level governance. For example, console manufacturers and major PC storefronts enforce content policies, review moderation processes, and in some cases, disable live broadcast functions for unverified or underage accounts. Such internal controls go well beyond the measures applied in most other online environments. Ukie is therefore concerned that Ofcom's proposals may inadvertently penalise services that are already safe by design, while creating unnecessary burdens for small and medium-sized studios that lack the capacity to rebuild technical systems multiple times per year. Chapter 22 of Ofcom's Combined Impact Assessment acknowledges that implementation costs for livestreaming measures may be significant, but it underestimates the true financial and operational impact on the video games sector. For many of our members, particularly those with complex or multi-platform titles, these costs would divert investment away from innovation and player experience without demonstrable safety benefits. In light of this evidence, Ukie strongly urges Ofcom to recognise that livestreaming in video games presents a distinct and comparatively low-risk use case. Ofcom should prioritise stability by allowing the current codes to be fully implemented and evaluated before layering new measures on top. Any further obligations should be proportionate, risk-based, and aligned with the principle of regulatory certainty to enable companies to plan and deliver meaningful safety improvements over time. Throughout this consultation, Ukie and its members will continue to stress the importance of evidence-led regulation. We welcome Ofcom's recent engagement with the sector and look forward to further dialogue aimed at ensuring that future measures reflect the operational realities, established safeguards, and proven effectiveness of the video games industry's safety-by-design approach.

Question	Your response
Question 2: Do you have further evidence regarding the benefits to users or children from livestreaming?	Livestreaming can bring a wide range of social, creative, and educational benefits, especially within the carefully managed environments that are typical of video games services. When designed and moderated appropriately, livestreaming helps to build community, strengthen digital literacy, and encourage self expression. For young people in particular, these activities can promote confidence, collaboration, and creative thinking. Video games livestreaming is distinct from livestreaming on social media because it takes place within structured and moderated settings that already include built in safety tools. Many of these environments are closed or community based rather than public, which greatly reduces risk. Livestreaming within video games has been shown to provide clear social benefits by connecting players with shared interests and helping them form meaningful friendships. Research by the National Literacy Trust in 2021 found that video games play a significant role in supporting young people's social connection and wellbeing, particularly during periods of isolation such as the Covid-19 pandemic. The study, *Video Games and Literacy: The Benefits of Playing Games for Children and Young People's Literacy and Wellbeing*, reported that 79 per cent of young people who played games said it helped them feel part of a community, while 65 per cent said gaming allowed them to spend time with friends or family. The research also highlighted that playing and talking about games encouraged communication, creativity, and shared learning, with many participants engaging in reading, writing, and problem-solving activities linked to their favourite games. These findings underline that interactive and livestreamed play can be an important positive force in young people's lives, fostering both social belonging and the development of digital literacy skills. Livestreaming is also a valuable educational tool. Through interactive play, it encourages curiosity and helps children to learn about teamwork, design, and problem solving. Initiatives such as Digital Schoolhouse have successfully used livestreaming to support workshops that promote creative computing and teamwork among school pupils. These programmes teach children to understand digital communication, respect for others, and responsible

Question	Your response
	online participation, which aligns closely with the aims of the Online Safety Act and the protection of children's wellbeing online. Livestreaming can also support mental health and confidence building. Organisations such as Safe in Our World host community streams that create open, supportive spaces for discussion about wellbeing and player experience. For many young people, the opportunity to create or participate in a stream can foster empathy, creativity, and social confidence. The video games industry has also built robust technical and parental control systems around livestreaming. As mentioned previously, publishers have terms that restrict livestreaming features for under eighteen accounts by requiring active parental approval. In these spaces, reporting tools, moderation systems, and session based communication are standard practice. As a result, livestreaming within video games takes place in a managed, responsible, and educationally valuable setting. For these reasons, Ukie encourages Ofcom to recognise the positive role that livestreaming plays in the video games ecosystem. Any new requirements should protect users without preventing the social and educational benefits that livestreaming provides. A proportionate and evidence based approach is essential to ensure that regulation supports both safety and creativity in digital play. Overly restrictive regulation may undermine these benefits. For example, if human moderation were mandated for all livestreams, smaller platforms and independent developers might have to disable the feature entirely, reducing access to these valuable creative opportunities. A balanced approach, recognising the positive educational and social impact of livestreaming, would better serve children's interests while ensuring that proportionate safeguards remain in place.
Question 3: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members share Ofcom's commitment to making online environments safer for all users, especially children. However, we do not agree with the current proposals, not just livestreaming but the wider proposals being consulted on, because they introduce another round

Question	Your response
	of significant regulatory changes before the earlier codes of practice have even been fully implemented or assessed. Our members have already invested substantial resources to meet the requirements set out in the Illegal Harms and Children's Safety Codes of Practice. These frameworks were only finalised recently, and many services are still completing the technical and organisational work needed for compliance. Introducing additional obligations at this stage undermines regulatory stability and creates confusion across the sector. The result is a situation in which companies are forced to rewrite risk assessments and redevelop compliance systems before the previous codes have even come into force. This approach creates uncertainty and costs that are far higher than Ofcom appears to recognise. Such constant revision of expectations makes long term planning impossible. Businesses cannot confidently plan product development, investment, or user safety improvements when they must repeatedly adapt to a moving set of requirements. For large publishers with multiple user to user services, this cycle has already occurred twice as Ofcom moved from draft to final versions of the earlier codes. Repeating that process again so soon is neither fair nor sustainable. For small and medium sized companies, which make up the overwhelming majority of the United Kingdom's video games sector, this instability risks diverting resources away from innovation and from improving player experience. Ofcom's approach also fails to reflect the practical realities of implementation. The proposed three month transition period between publication of final codes and enforcement is not workable. Implementing new safety measures, updating risk assessments, retraining moderators, and testing systems properly requires far more time. A minimum implementation period of six to nine months would be far more realistic and would allow for meaningful compliance. We are further concerned that the proposals are overly prescriptive. The requirements around livestreaming, proactive technology, and user sanctions assume that all services operate in the same way. Video games environments are fundamentally different from social media and

Question	Your response
	require a more flexible approach. For example, the expectation that human moderators must be available whenever livestreaming occurs is excessive and fails to consider that most video games already include strong built in controls, restricted communication channels, and automated reporting. Mandating such measures across the board would introduce privacy concerns and significant new costs for very limited benefit. Similarly, Ofcom's expectations regarding proactive technology and hash matching go beyond what current technology can deliver. These tools can generate false positives and are not always effective in detecting the types of content Ofcom identifies. Forcing the use of third party hash databases could lead to the unnecessary removal of legitimate content and impose substantial engineering burdens. Providers should retain flexibility to rely on internal systems that are already proven to be effective and reliable. We are concerned that the livestreaming proposals would impose blanket obligations that do not reflect how livestreaming operates in video games. The requirement for human moderators to be available whenever users can livestream and the new imminent harm reporting mandate would be onerous for services where livestreaming is an ancillary feature, controlled by design, and already supported by effective reporting and parental tools. We also have reservations about the proposal to remove broad interaction features from all child streams rather than targeting higher-risk contexts. These issues relate directly to Ofcom's measures ICU C16, ICU D17, and ICU F3. Lastly, the proposed obligations on user sanctions risk overreach. Many Ukie members already operate clear, proportionate systems of warnings, suspensions, and bans, often working directly with law enforcement agencies such as the National Centre for Missing and Exploited Children. Requiring companies to retrofit additional processes where effective ones already exist would waste resources without improving user protection. Ukie therefore strongly urges Ofcom to pause these proposals until at least summer of next year. This would give the earlier codes of practice time to take effect and allow

Question	Your response
	Ofcom to evaluate their impact before layering new requirements on top. A stable, predictable, and proportionate regulatory environment is essential if companies are to deliver meaningful safety improvements while continuing to innovate and grow the sector.
Question 4: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie and its members do not agree with Ofcom's assessment of the impacts and costs associated with the proposed additional safety measures. The consultation significantly underestimates the financial, technical, and operational burden that these proposals would place on the video games industry. It also overlooks the cumulative effect of ongoing regulatory revisions and the instability that constant policy changes create for service providers. In Chapter 22 of the consultation's Combined Impact Assessment, Ofcom acknowledges that compliance with the proposed measures may require investment in moderation, engineering, and training, but the cost estimates presented do not adequately reflect the complexity of implementation across live services. The measures proposed in ICU D17 and ICU C16 on livestreaming, for instance, would require providers to ensure that human moderators are available whenever users can stream, and to build new reporting functions to flag imminent risks of harm. These requirements are operationally demanding and costly. They would also require reengineering of systems that are already compliant with the existing codes. For larger publishers operating several user-to-user services, each with different functionalities, this could mean multiple parallel development and testing projects. For smaller studios, the level of technical and human resource investment required is likely to be unmanageable. Similarly, the new proposals relating to proactive technology (ICU C11 and PCU C9) would obligate providers to assess and, where feasible, deploy automated tools to detect illegal or harmful content. These systems are not only expensive to integrate but also remain technically limited in accuracy, producing high false positive rates. The cost of deploying, monitoring, and verifying such tools at scale goes far beyond the assumptions in Ofcom's impact analysis.

Question	Your response
	The proposed use of hash-matching technology for detecting intimate image abuse (ICU C14) and terrorism content (ICU C13) is also presented in the consultation as a relatively straightforward measure, but in practice it involves substantial computational cost, data storage, and content verification processes. Inaccurate matches can result in the wrongful removal of legitimate content, forcing additional manual reviews and further cost. Mandating third-party databases, as implied by the proposals, would create ongoing licensing costs and introduce privacy and data protection considerations not accounted for in Ofcom's estimates. Ofcom's cost analysis also fails to consider the indirect effects of policy churn. Many Ukie members have already implemented significant technical changes to comply with the Illegal Harms and Children's Safety Codes of Practice, which were finalised only months ago. Revisiting risk assessments and compliance systems again, before those codes have even been evaluated, imposes repeated cycles of cost and rework. The short implementation period of three months between final publication and enforcement, as stated in the consultation, further amplifies these pressures by forcing companies to reallocate staff and budgets from planned development projects to rushed compliance activity. For these reasons, Ukie and its members believe Ofcom's cost modelling is incomplete and unrealistic for the video games sector. We urge Ofcom to revisit its analysis with input from industry to ensure that cost assessments accurately reflect the complexity of technical delivery, to extend the implementation period to at least six to nine months, and to delay the introduction of new measures until the current codes have been fully implemented and reviewed. This would create a more proportionate and stable regulatory environment that supports effective safety outcomes while allowing the industry to innovate and grow.
Question 5: Do you have any views on the optimal design of reporting functions and choice categories for users to report content that depicts the risk	Ukie supports the principle that services should provide clear and effective mechanisms for users to report content that depicts or indicates a risk of imminent physical harm. However, we believe Ofcom's proposal in ICU D17,

Question	Your response
of imminent physical harm ? Include any evidence, such as, testing to optimise wording, design of tools to support users to submit accurate and timely reports and how these may be used to support moderation actions.	which would require all user-to-user services offering one-to-many livestreaming at medium or high risk to include a specific reporting mechanism for imminent harm, needs to be implemented in a proportionate and flexible way that recognises the diversity of services covered by the Online Safety framework. Ofcom's consultation sets out the intention that these new reporting tools should allow users to flag content such as self-harm, suicide attempts, or real-time violence during livestreams. While Ukie agrees that users should be empowered to act quickly in those circumstances, the optimal design of these functions depends heavily on the nature of the service and the user interface. For many video games services, livestreaming is either restricted, pre-moderated, or hosted on a separate platform with its own moderation tools. Imposing a single design model or set of reporting categories across all services would therefore not be practical. Additionally, if a video games from a developer is played on a platform and streamed on a non-games related forum such as social media, it would be useful from Ofcom to know who the party responsible to impose the additional duties would be. Our members' experience shows that the most effective reporting systems are those integrated into existing moderation workflows and aligned with the user journey. Within games environments, reporting is often embedded within a pause menu, player profile, or match summary screen, allowing users to report an incident without interrupting gameplay. To encourage accurate and timely reporting, it is crucial that interfaces remain simple, context-sensitive, and not overly technical. Industry research conducted by Epic Games and Activision, for example, shows that when reporting tools use plain, action-based language such as "Report harmful behaviour" or "Report safety concern", submission rates increase significantly compared to when users are presented with long lists of complex categories. Ukie members have also found that combining pre-defined categories with an open text option improves accuracy. Simple labels such as "Threat of violence", "Self-harm or suicide", and "Emergency risk" enable users to respond quickly while still providing moderators with

Question	Your response
	enough context to prioritise review. Where users are uncertain, having an option to select "Something else unsafe" ensures that potentially serious reports are still captured and assessed. The consultation suggests that these reporting tools could be used to support faster moderation and referral to law enforcement. Ukie agrees that this should be the goal, but this requires Ofcom to recognise the operational context in which games companies work. Most companies already maintain trusted relationships with law enforcement, including the National Crime Agency and the National Centre for Missing and Exploited Children, and have established escalation pathways for imminent threats. Integrating these existing mechanisms with new reporting categories is more efficient than building parallel systems. Finally, we note that Ofcom's guidance in Chapter 10 acknowledges that services should consider user privacy when designing reporting tools. Ukie welcomes this recognition and emphasises that any reporting process must avoid collecting unnecessary personal data or requiring identifiable information that could discourage users, especially children, from reporting concerns. Anonymous or pseudonymous reporting should remain an option wherever feasible. Ukie supports the overall goal of ICU D17 but urges Ofcom to allow flexibility in design. Reporting tools should be tailored to the structure of each service, tested for clarity and accessibility, and integrated into existing moderation systems. Ofcom should also consult industry before finalising recommended choice categories, to ensure that the language and functionality reflect how users actually experience and report harm within different types of online environments.
Question 6: Do you consider that there are alternative measures which would materially reduce the risks to users from livestreaming such as preventive safety by design frictions, prompts or restrictions? If so, please	Ukie and its members recognise the importance of reducing potential harms associated with livestreaming, particularly where there is a risk of imminent physical harm. However, we believe that the measures proposed by Ofcom in ICU D17, ICU C16, and ICU F3 are unnecessarily prescriptive and do not reflect the practical realities of how livestreaming operates within video games environ-

Question	Your response
detail them and provide evidence on the costs and efficacy.	ments. The same objectives can be achieved through alternative safety by design measures that are more proportionate, more effective, and far less costly to implement. The proposals in ICU C16 would require human moderators to be available whenever livestreaming takes place, while ICU F3 would impose blanket restrictions on interaction during livestreams hosted by children. These measures, while well intentioned, would be disproportionately burdensome for services that already embed robust safety systems. For games companies, livestreaming is typically an ancillary function, not a central part of the user experience. In many cases, communication and broadcasting capabilities are limited, structured, or pre-moderated. Applying a one-size-fits-all rule across such diverse environments risks undermining innovation while failing to deliver measurable safety improvements. There are more effective ways to meet the intent of these proposals through preventive design features that are already standard across much of the industry. For instance, parental controls and account-level settings can restrict access to livestreaming for children, require active consent from parents or guardians, or limit the audience to pre-approved friends lists. Systems such as these are widely used on platforms. They allow services to achieve the same protective outcomes as Ofcom's proposals, but at a fraction of the cost and without imposing unnecessary operational burdens. Other preventive tools include short broadcast delays and automated detection of keywords or behaviours associated with distress or violence. These systems, already in use across major games platforms, enable moderators to review and intervene in near-real time without requiring constant human oversight. When combined with clear in-service reporting functions (such as those discussed in ICU D17) these measures provide a multi-layered safety framework that is adaptable and cost-effective. Moreover, many services already integrate safety prompts or "friction" points that remind users of appropriate conduct before or during a stream. Examples include pre-stream checklists for privacy settings, pop-up messages warning against sharing personal details, and

Question	Your response
	automated notifications encouraging users to report concerning content. The costs of implementing these preventive features are significantly lower than Ofcom's assumptions in the Combined Impact Assessment. The majority of these tools build upon existing systems such as moderation workflows, reporting dashboards, and parental control frameworks. They do not require continuous human staffing or major new infrastructure. For smaller studios, this approach provides a realistic pathway to compliance without diverting critical resources from game development or player support. Ukie's concern remains that Ofcom's current proposals risk moving the goalposts once again, introducing new requirements before the existing codes of practice have been implemented or evaluated. A more effective strategy would be to allow time for current measures to take effect, assess their impact, and then work with industry to refine safety by design principles based on real evidence.
Question 7: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members support Ofcom's objective of ensuring that livestreaming by children is safe, but we do not support the blanket restrictions proposed under ICU F3. The proposal would prevent children from receiving comments, reactions, gifts, or recordings on any livestream, regardless of context or risk level. This one-size-fits-all approach does not reflect the way livestreaming functions in video games, where the activity is typically limited, community-based, and already governed by robust safeguards. Within games, livestreaming is a form of play, not a form of public broadcasting. It takes place within controlled environments with restricted audiences, often among friends or family. Platforms such as PlayStation Network, Xbox Live, and Nintendo Switch Online already disable livestreaming for under-18s by default unless parental consent is provided. Where enabled, these platforms apply additional limits on visibility, chat, gifting, and audience size. These protections are reinforced by the statutory PEGI system, which has legally governed age ratings and online

Question	Your response
	safety standards since 2012. The PEGI Code of Conduct requires signatories to implement clear moderation and parental control mechanisms for all online features, including communication and livestreaming. This framework already ensures that livestreaming functions are age-appropriate and effectively moderated. Ukie therefore considers the ICU F3 proposal unnecessary and disproportionate for the games industry. It risks removing positive and creative social interaction (core elements of modern play) without demonstrable evidence of harm in this context. Instead of mandating universal feature removal, Ofcom should recognise and build upon the safety-by-design model already established in the games industry, which delivers the same outcomes through targeted, evidence-based safeguards. Ukie supports Ofcom's objectives but not the current approach. We recommend that Ofcom reframes its proposals to focus on outcomes rather than prescriptive processes, scales obligations based on risk and functionality, and allows sufficient time for implementation. This would ensure regulation remains proportionate, effective, and sustainable for the UK's video games industry, which has a long-standing record of designing for safety and delivering strong protections for players of all ages.
Question 8: If you are a service provider, what measures do you currently undertake to moderate livestreams and protect children who undertake livestream broadcasts, and what is your evidence on the effectiveness of such measures?	Video games companies already operate extensive moderation and child-safety systems that meet, and in many cases exceed, the aims of ICU F3. Livestreaming for children is restricted by default across all major platforms, and can only be activated with verified parental consent. When enabled, audience visibility is tightly controlled, chat and reactions are filtered, and gifting is limited or disabled. Games are built on safety-by-design principles. They incorporate parental dashboards that allow guardians to approve livestream settings, review play activity, and manage permissions. Many services also use preventive prompts that remind young users about privacy and respectful conduct before a broadcast begins. Real-time moderation tools monitor chat for high-risk language,

Question	Your response
	while clear reporting mechanisms allow players and parents to flag inappropriate content or behaviour immediately. Across major video games platforms, livestreaming moderation and protection mechanisms typically include: **1. PEGI age ratings and Code of Conduct compliance:** Since 2012, the PEGI system has had legal status in the UK under the Video Recordings Act, with statutory ratings administered by the Games Rating Authority. PEGI ratings cover not only in-game content but also online functionality, including communication, user interaction, and sharing tools such as livestreaming. Every publisher and platform that adopts PEGI commits to a robust Code of Conduct requiring responsible advertising, parental guidance, age-appropriate access, and user protection online. PEGI regularly audits compliance and can issue sanctions or financial penalties where standards are not met. This system provides a formal, transparent framework that already achieves the outcomes Ofcom seeks through its livestreaming proposals. **2. Parental controls and age gating:** All major platforms include granular parental controls that manage whether a child account can access livestreaming features at all. These are disabled by default for underage accounts and can only be enabled through verified parental consent. Where permitted, livestreaming is restricted to small audiences, typically consisting of approved friends or contacts, and chat features are limited or pre-moderated. **3. Restricted communication and contextual design:** Livestreaming in games is fundamentally different from open broadcasting. It is designed to enhance shared play and collaboration rather than provide a platform for general communication. Text or voice chat is session-based, ephemeral, and usually limited in scale. Many companies deploy text and voice filters to automatically remove or block harmful or explicit language, ensuring that players—particularly children—are shielded from inappropriate content during live sessions. **4. Automated moderation and behaviour detection:** Games companies deploy advanced AI moderation systems to detect risks in real time. These tools analyse chat

Question	Your response
	and voice communications for harmful patterns, keywords, or aggressive language. For example, Activision's integration of Modulate's "ToxMod" in *Call of Duty* has led to a 67 per cent reduction in repeat abusive behaviour. These systems enable effective monitoring and escalation without requiring constant human oversight. **5. Reporting and escalation mechanisms:** Clear reporting tools are integrated into all major games and platforms, allowing players to flag harmful content or behaviour quickly and easily. Reports are triaged by trained moderation teams and escalated where necessary to platform-level safety departments or external authorities. The industry works in partnership with trusted organisations such as the National Crime Agency, the Internet Watch Foundation, and the National Centre for Missing and Exploited Children to ensure that criminal material is identified and referred promptly. **6. Broadcast delays, prompts, and preventive frictions:** Short delay buffers are often built into livestreaming features, enabling moderation intervention before potentially harmful content becomes visible. Pre-stream prompts remind users about privacy, consent, and appropriate behaviour. For child users, prompts can require confirmation of safe settings—such as restricted audiences and chat limits—before a stream begins. These frictions encourage reflection and significantly reduce impulsive or risky broadcasting behaviour. **7. Education and parental engagement:** Ukie and its members actively promote awareness and parental confidence through initiatives such as *Ask About Games* and *Get Smart About P.L.A.Y.* These programmes provide parents and carers with accessible guidance on using parental controls, managing livestream settings, and supporting healthy play. They complement the PEGI system and ensure that families understand the tools available to them. **Evidence of effectiveness:** The effectiveness of these combined measures is well documented. According to the National Centre for Missing and Exploited Children's 2022 CyberTipline report, of more than thirty-two million global reports of child sexual abuse material, only 8,200 originated from video game

Question	Your response
	platforms—representing roughly 0.00025 per cent of total reports. This extremely low figure reflects the success of the video games industry's multi-layered safety systems. Moreover, internal company data show that incidents involving livestreamed harm in games are rare, and when they do occur, they are identified and addressed rapidly through established moderation workflows. The PEGI framework also ensures that content moderation and online safety are consistent across all PEGI-rated titles. PEGI's mandatory "Online Safety" icon and associated criteria ensure that companies provide appropriate user reporting, content moderation, and parental oversight tools. This statutory regime already serves as a powerful safeguard for livestreaming content.
Question 9: Do you consider that there are alternative measures which would materially reduce the risks children face when livestreaming, both in general and in relation to operation of the supporting functionalities of comments, reactions, gifting and content capture? If so, please detail them and provide evidence on the costs and efficacy.	Yes. Ukie and its members believe there are more proportionate and technically feasible alternatives to ICU F3 that achieve the same safety outcomes while preserving the positive aspects of online play. Protective defaults can limit child livestreams to friends-only audiences and disable discoverability unless a parent or guardian opts in. Comments can be rate-limited or filtered by automated moderation tools, reactions restricted to pre-approved icons, and gifting placed behind spending caps and parental approval. Many services already employ pre-stream prompts reminding children not to share personal information, and visible watermarks to deter screen capture and redistribution. These measures are cost-effective because they build on existing infrastructure - parental controls, moderation pipelines, and purchase systems - rather than requiring continuous human oversight. They also maintain opportunities for creativity and connection, essential to healthy online play. Ukie supports a regulatory model that encourages such layered, safety-by-design approaches instead of mandating universal feature removal. This ensures proportionality, respects the diversity of services, and reinforces the UK games industry's strong track record in child protection.

Question	Your response
Question 10: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie and its members do not agree with Ofcom's cost assessment for ICU F3. The analysis underestimates the engineering and operational resources needed to disable or redesign livestream features across live services, and it does not reflect the cumulative burden of repeated regulatory change. Implementing ICU F3 would require significant redevelopment of video, chat, and interface systems across multiple platforms. Each modification must undergo quality assurance, certification, and localisation, representing substantial time and expense. For smaller studios, such requirements could divert limited resources from core safety improvements already underway under the existing codes. The proposals also ignore the broader economic impact. Many livestreaming features are integral to community engagement and esports events. Removing them entirely for all under-18s would diminish participation and innovation in a sector that already leads in online safety. Ofcom's suggested three-month implementation window is unrealistic. A minimum of six to nine months is needed to plan, develop, test, and deploy compliant updates while maintaining service stability. Ukie urges Ofcom to reassess its cost model to reflect real development cycles and to recognise that the existing PEGI-backed, safety-by-design framework already mitigates the risks ICU F3 seeks to address. Proportionate regulation should support the continuation of these proven systems rather than impose costly, prescriptive changes with limited additional benefit.
Question 11: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members support the objective of reducing serious harms, but we do not agree with the proposals as drafted under ICU C11 and PCU C9, and ICU C12 and PCU C10. The measures are framed in a way that risks turning outcome guidance into de facto mandates to deploy automated tools wherever they exist. Ofcom's current proposal would require every large or high-risk service to "assess and, if feasible, deploy proactive technology," regardless of whether the service's design actually allows such harms to occur at meaningful scale. This is neither

Question	Your response
	proportionate nor supported by available evidence. Communication in games is often limited, contextual, and ephemeral, focused on teamwork and gameplay rather than social broadcasting. As such, the scope for disseminating illegal or harmful material is already low. Industry experience shows that layered safety by design, supported by targeted automation and clear reporting, delivers better results than broad obligations to assess and deploy every available tool. For example, voice and text analysis used alongside graduated enforcement has reduced repeat abusive behaviour in large titles, but only where tools are tuned to the service and supported by human oversight and appeals. We therefore support an approach that is proportionate, service specific, and technology neutral, and that recognises the statutory PEGI framework and existing moderation standards as part of the compliance picture.
Question 12: Do you have any comments on the Proactive Technology Draft Guidance?	Ukie welcomes Ofcom's intention to clarify expectations but believes the draft guidance requires more precision. It must recognise the limitations and potential harms of proactive technologies, especially false positives and privacy intrusions. The guidance should establish minimum accuracy and transparency thresholds and recognise that not all harms can be effectively detected through automation. For example, technologies designed to detect grooming, suicide encouragement, or harassment still struggle to interpret context, tone, and language diversity accurately. Automated tools can misclassify harmless interactions, which increases the burden on human moderators and creates user trust issues. These tools also rely on access to sensitive communications data, raising questions about proportionality and data protection compliance. A more effective approach would be to encourage voluntary adoption of proactive tools where demonstrably effective, while recognising that many games already use layered systems - combining user reporting, in-game controls, and real-time moderation - that achieve the same objectives. Ofcom should also provide clarity on how internal, service-specific moderation systems will be

Question	Your response
	treated, since many companies have developed highly effective bespoke solutions that outperform off-the-shelf products.
Question 13: Do you agree with the harms currently in scope of these measures? Are there any additional harms that these measures should capture? Please provide the underlying arguments and evidence that support your views, including evidence regarding the availability of accurate and effective proactive technology.	NA
Question 14: Do you agree with who we propose should implement these measures? Are there any other services that should be captured for some or all of the relevant harms?	Ukie does not agree with applying the same expectations to all services based purely on user numbers or theoretical risk levels. The proposed thresholds of 700,000 UK monthly users does not account for the vast diversity of service models and risk profiles. Many large-scale games have highly restricted communication systems and advanced safety features, meaning that their actual exposure to user-generated harm is minimal. Applying the same requirements to these services as to open social platforms would not be proportionate. Instead, Ofcom should assess obligations based on demonstrable risk factors: the nature of user interaction, the openness of the communication environment, and the efficacy of existing safety systems. For example, multiplayer games with structured or team-based chat already operate within controlled, purpose-specific systems and should not be subject to the same standards as public, content-sharing platforms. Smaller studios also need to be protected from overreach. Implementing and evaluating proactive tools requires specialised engineering, data science, and compliance capacity that small and micro studios simply do not have. Without proportional thresholds and sufficient lead time, these proposals risk hindering innovation and overburdening responsible developers.

Question	Your response
Question 15: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie and its members do not believe Ofcom's cost assessment fully reflects the operational reality of implementing these proposals. Integrating proactive technologies is not a simple plug-and-play process—it requires vendor review, data protection assessments, localisation, quality assurance, and continual calibration. Every iteration must be tested across multiple hardware platforms and service versions, especially where voice or text moderation is embedded in gameplay. False positives also drive up costs significantly, requiring additional moderators, appeals processes, and data storage. Engineering teams must rework systems architecture to integrate third-party tools and ensure they align with existing privacy-by-design frameworks. For multi-platform titles, the same work must often be repeated several times to meet platform certification requirements. Ofcom's assumption that such systems can be deployed within short timeframes or at modest cost is unrealistic. Based on industry feedback, a six to nine month lead time is the minimum necessary to implement, test, and certify any new technology safely and without compromising live service stability. The cumulative effect of introducing overlapping regulatory requirements before previous codes have been embedded creates a moving target for compliance, forcing developers to continually divert resources from core product development and innovation. This undermines both the competitiveness of the UK games sector and the effectiveness of the regulation itself. Ukie therefore urges Ofcom to adopt a stable, proportionate, and evidence-led approach allowing sufficient time for evaluation of the existing Codes before mandating new, resource-intensive measures that offer limited additional safety benefit.
Question 16: Do you agree with our proposal?. Please provide your reasoning, and if possible, provide supporting evidence.	Ukie members agree that combating illegal content is a critical priority, but urge Ofcom to calibrate its expectations to the technological and operational realities of the video games sector. The industry already takes a proactive stance in preventing and reporting illegal material, particularly child sexual abuse content. Companies work

Question	Your response
	closely with the National Crime Agency, the Internet Watch Foundation, and NCMEC, ensuring swift identification and removal when incidents occur. However, Ofcom's proposals risk overreach. Expanding mandatory proactive detection across all priority harms without regard for service type or communication functionality would impose unsustainable demands. For example, most games do not support image or video uploads, making the likelihood of illegal content dissemination extremely low. Applying uniform obligations would divert resources from higher-impact safety initiatives. Current detection systems for certain categories, such as terrorism or fraud, remain underdeveloped and prone to error. Mandating their use prematurely could lead to unjustified user sanctions and significant engineering burdens. Inferring illegality without direct evidence risks undermining trust in moderation processes and could inadvertently capture legitimate communities that use stylised or coded language for non-illicit purposes (for example, competitive teams, creators, or fandom groups). Ofcom should therefore ensure that any such guidance remains exceptional, used only where there is verifiable evidence of criminal intent, and always accompanied by a clear appeals process. Proportionate and evidence-led regulation remains essential to preserving safety and user rights in equal measure. Ukie members support an evidence-based approach: one that differentiates between service types and focuses on demonstrable risk. By aligning regulatory requirements with the actual capabilities and risk profiles of video games services, Ofcom can ensure effective, proportionate protection for users without stifling innovation or overwhelming smaller developers.
Question 17: Do you have any evidence relevant to the examples given?	Ukie members recognise the role of hash matching in identifying and preventing the circulation of known illegal content, particularly child sexual abuse material (CSAM). However, the sector has strong concerns about Ofcom's proposal to expand mandatory use of hash matching across a wider set of harms, including intimate image

Question	Your response
	abuse, terrorism, and extreme violence. Current technologies are not sufficiently reliable or scalable to justify such a broad mandate. Game platforms use multi-layered safeguards that make "breadcrumbing" behaviours difficult to sustain. Usernames, profile images, and chat bios are automatically filtered for prohibited terms, and suspicious accounts are proactively flagged or blocked. Parental tools on PlayStation, Xbox, Nintendo and PC storefronts restrict or entirely disable child accounts from interacting with unknown users or joining public groups. Furthermore, game publishers maintain direct channels with law enforcement agencies, including the Internet Watch Foundation and the National Crime Agency, to swiftly remove and report any suspected illegal material. This layered prevention model demonstrates that the risks Ofcom identifies are not representative of the typical user experience in video games environments. Mandating new inference-based judgements would not materially improve detection rates in these already low-risk contexts, but would introduce significant moderation overhead and potential error. Ukie members therefore recommend that Ofcom acknowledge the current technical limitations and permit flexible compliance. Services should be allowed to rely on internal systems where these demonstrably achieve equivalent safety outcomes. Ofcom should also work with the sector to establish transparent auditing standards for hash databases to ensure quality, privacy, and accountability before mandating their use.
Question 18: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie does not agree that Ofcom's assessment accurately reflects the operational and legal implications of the proposed amendments. Inference-based judgements without direct content review would require substantial reconfiguration of moderation systems and retraining of moderation teams. Engineering and trust-and-safety functions would need to implement new workflows to analyse profile metadata, correlate reports, and escalate cases (activities not currently part of standard processes).

Question	Your response
	Each new moderation layer introduces additional costs: developing or licensing automated filters, integrating them across multiple platforms, and ensuring compliance with data protection and privacy law. For smaller or mid-sized studios, these costs are disproportionate to the minimal risk presented by their services. There are also non-financial impacts, including the increased risk of wrongful takedowns and user appeals, which can erode community trust and lead to reputational harm. From a legal standpoint, inferring criminal activity without direct evidence raises questions around data processing legitimacy and freedom of expression, particularly in private or semi-private channels. Ofcom's proposal also assumes technical feasibility where it may not exist—many game systems cannot review group metadata without violating core privacy-by-design principles embedded in platform architecture. Ukie therefore urges Ofcom to reconsider this proposal and focus instead on fostering evidence-sharing with law enforcement, improving intelligence flows, and supporting voluntary use of proven detection systems where risk and technical feasibility justify it. This would strengthen child protection outcomes while maintaining proportionality, privacy, and legal certainty for compliant low-risk sectors such as video games.
Question 19: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	NA
Question 20: Do you have any evidence on the relative efficacy of third-party and internal databases for image-based IIA content?	NA
Question 21: Do you consider this measure to be effective for file-sharing and file-storage services? Please explain your reasoning and, if possible, provide supporting evidence.	NA

Question	Your response
Question 22: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	NA
Question 23: Do you consider this measure to be effective for large general search services? Please explain your reasoning and, if possible, provide supporting evidence.	NA
Question 24: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	NA
Question 25: Do you have evidence regarding the accuracy and effectiveness of hash matching solutions for detection of terrorism content specifically (including their false positive and false negative rates);	NA
Question 26: Do you have evidence on the extent to which a hash matching solution can identify terrorism content accurately when applied in different contexts from that in which the hash was created, noting the potential implications for freedom of expression;	NA
Question 27: Do you have a view on the degree of human oversight required to support the use of hash matching in relation to terrorism content?	NA
Question 28: Do you have evidence or views on the impact assessment (including costs) associated with imple-	NA

Question	Your response
menting and maintaining hash matching technology for the detection of terrorism content (such as the impacts and costs of setting up an internal database, connecting to an external provider, and moderation costs).	
Question 29: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members fully support the goal of reducing and removing child sexual abuse material (CSAM) online and recognise the importance of extending safety requirements to higher-risk services. However, we do not believe that Ofcom's proposed amendment to ICU C9, namely extending mandatory hash-matching to additional high-risk user-to-user services whose principal purpose is the hosting or dissemination of regulated pornographic content, is relevant to, or proportionate for, the video games sector. The games industry is not a driver or host of CSAM and does not operate services designed for adult or pornographic content. Communication in video games is typically limited, transient, and closely moderated. Interactions between players are often purpose-driven and occur within structured, closed environments designed primarily for gameplay. As such, there is minimal opportunity for the sharing of illegal images or persistent media files. Existing data supports this view. The National Centre for Missing and Exploited Children (NCMEC) recorded only 8,200 reports of CSAM from all global games platforms in 2022 - representing less than 0.001 per cent of the total 32 million reports. This demonstrates that games companies' longstanding safety-by-design measures, combined with rigorous moderation and reporting systems, have proven highly effective at preventing and removing harmful material. Extending the hash-matching requirement to sectors already demonstrating low or negligible risk would not improve detection rates but would divert resources away from the continuous improvement of proven safety systems. Instead, Ofcom should ensure that the measure remains tightly focused on genuinely high-risk services, such as those whose core business model involves hosting or sharing explicit media, and not inadvertently extend the

Question	Your response
	definition to capture low-risk entertainment platforms like video games.
Question 30: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie does not agree that Ofcom's impact assessment accurately reflects the real costs and feasibility challenges associated with implementing or extending hash-matching technologies. The technical, operational, and financial implications are considerable. Even for companies already using automated detection tools for moderation, integrating a full-scale CSAM hash-matching system would require extensive infrastructure upgrades, additional compliance frameworks, and specialised staff training. Hash-matching databases must be regularly synchronised with trusted third-party sources, tested for accuracy, and validated against local data protection requirements. Each integration increases computational load and moderation overhead, particularly for multi-platform games that must deploy systems across console, PC, and mobile environments. False positives remain a significant risk and can generate large volumes of manual review work, which is especially burdensome for smaller studios or start-ups. Crucially, Ofcom's assumption that these measures can be deployed within short timeframes and at moderate cost does not reflect the experience of regulated companies. Implementation timelines of at least six to nine months are typically needed for safe deployment and testing, especially when factoring in certification by platform holders. For smaller developers, these costs would be disproportionate to the negligible risk they pose in this area. Ukie therefore urges Ofcom to ensure that the amended ICU C9 remains strictly targeted at services genuinely at risk of hosting or disseminating CSAM, and that any future expansion of scope includes a clear proportionality test. This will help ensure that regulatory requirements are both effective in protecting children and sustainable for the UK's diverse creative sectors

Question	Your response
Question 31: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	NA
Question 32: Do you have evidence on what types of content are typically recommended to users as part of concerted foreign interference activity;	NA
Question 33: Do you have evidence on whether services track the extent of algorithmic amplification, such as impressions and reach, of content that is later deemed illegal/violating. If so, do they (or does your service) use this information to enhance the safety of their systems?	NA
Question 34: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	NA
Question 35: Are there any impacts of the proposed measure that we have not identified? Please provide the rationale and any supporting evidence for your response.	NA
Question 36: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members strongly support decisive measures to prevent the sharing and circulation of child sexual exploitation and abuse (CSEA) content online. We agree that individuals found to have generated, uploaded, or shared such material should be subject to strict enforcement, including account bans and proactive steps to prevent re-entry. This is consistent with the long-standing practices across the video games industry, where users who violate terms of service through harmful or illegal conduct are routinely removed and blocked. However, we believe Ofcom's proposal under ICU H3 must remain proportionate and flexible, recognising that

Question	Your response
	different services have distinct risk profiles and operational models. Games environments are not comparable to open social media platforms. They are highly moderated, structured around gameplay rather than general communication, and typically employ safety-by-design principles that limit opportunities for such offences. We also note that permanent bans are already standard practice across major platforms and publishers. Companies such as PlayStation, Xbox, and Nintendo use account-level and hardware-level restrictions, while PC storefronts and online games employ robust digital identity and behavioural tracking systems to prevent reoffending. These approaches are often coupled with escalation pathways to law enforcement agencies like the National Crime Agency and NCMEC. In this context, Ofcom's proposal largely formalises what the industry already delivers voluntarily. The key concern is ensuring that regulatory requirements remain flexible enough to accommodate existing, proven enforcement models without imposing unnecessary duplication or additional reporting burdens.
Question 37: What is your assessment of the options we set out in relation to the treatment of child users and which option do you consider to be most appropriate? Please provide any supporting evidence to support your arguments.	Ukie agrees with Ofcom that the treatment of child users requires particular care and nuance. While it is vital to remove harmful material swiftly, automatic or indiscriminate bans risk penalising children who may be victims rather than perpetrators. There are instances where a young person is coerced into sharing self-generated CSAM or manipulated into inappropriate behaviour. In such cases, a permanent ban could compound the harm, especially where the child may already require safeguarding support. We therefore support a case-by-case, evidence-based approach that allows services to exercise discretion, with mandatory escalation to child protection authorities when there is reasonable suspicion of coercion or exploitation. Existing industry frameworks already accommodate this nuance. Games companies routinely work with law enforcement and specialist organisations to differentiate between malicious activity and safeguarding cases. For example, many services implement layered sanctions, such as temporary suspensions combined with referral to

Question	Your response
	in-game safety teams or external child protection agencies. Ofcom's guidance should therefore prioritise context and proportionality. The presumption of a permanent ban should remain for verified adult offenders, but services should retain discretion to apply alternative interventions for children, guided by input from safeguarding professionals and the relevant authorities.
Question 38: Do you agree with our assessment of the impacts (including costs) associated with this proposal? Please provide any relevant evidence which supports your position.	Ukie agrees that the cost of implementing user bans and re-entry prevention measures is modest for larger services, as these systems are already in place across most games platforms. The industry has long employed account, device, and behavioural identifiers to detect repeat offenders, with internal compliance systems that escalate serious incidents to law enforcement. However, Ofcom's assumption that this measure carries low implementation cost for all providers does not account for the diversity of the sector. Smaller studios, start-ups, and micro-developers may not operate dedicated moderation or identity infrastructure and would need to develop or purchase third-party tools to meet compliance. For these businesses, even low-frequency enforcement processes can require meaningful resource investment in training, policy design, and reporting. In practical terms, the primary challenge is not technical feasibility but proportionality and clarity. Services need guidance on what constitutes "reasonable steps" to prevent a banned user's return. For example, while console and PC ecosystems can rely on verified accounts, many smaller online games lack persistent identity systems and cannot track users beyond usernames or IP addresses. Ofcom should explicitly acknowledge these limitations and clarify that compliance can be achieved through proportionate steps, such as account-level bans and prompt reporting to law enforcement. Overall, Ukie supports the intent of the proposal but calls for clear, flexible guidance that recognises the diversity of service design across the online ecosystem, ensures the

Question	Your response
	safeguarding of child victims, and avoids unnecessary duplication of existing, effective enforcement measures already embedded within the video games industry.
Question 39: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members support the principle that services should take consistent and proportionate action against users who share illegal or harmful content. The video games industry has, for many years, maintained robust sanctions policies to protect players and maintain safe environments. Every major online games service already operates a graduated sanctions model, ranging from education and temporary restrictions to permanent account or device bans for serious or repeat offences. This aligns with the intent of Ofcom's proposed ICU H2 and PCU H2 measures. However, we believe that Ofcom's proposal should remain flexible and proportionate to the scale, nature, and functionality of each service. Video games differ significantly from open social platforms: communications are limited, often ephemeral, and typically contextual to gameplay. As such, the risk of repeated dissemination of illegal or harmful content is very low. A one-size-fits-all model for sanctions policy would not reflect these differences and could impose unnecessary administrative burdens, especially on smaller developers and studios. Existing industry practice already delivers the outcomes Ofcom seeks. For example, all PEGI-rated platforms and publishers apply code of conduct enforcement through clear and transparent policies, which are regularly reviewed and monitored. Companies also escalate severe incidents, including illegal content or suspected grooming, directly to law enforcement bodies such as the National Crime Agency or the Internet Watch Foundation. The effectiveness of these systems is evident in the very low rates of illegal activity reported within games services compared to other online sectors. Ukie therefore supports Ofcom's objective but urges the regulator to avoid prescriptive requirements for sanctions design or structure. Providers should retain discretion to determine proportionate measures appropriate to their platform, with guidance focused on principles of fairness,

Question	Your response
	transparency, and effectiveness rather than rigid operational models.
Question 40: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie does not agree that Ofcom's assessment fully captures the costs associated with implementing and documenting sanctions policies, particularly for small and medium-sized companies. While larger studios and platform holders already operate comprehensive moderation and enforcement systems, many smaller online services manage these functions manually or through limited automation. Formalising, auditing, and reporting sanctions policies under the proposed Codes would therefore require additional resourcing, policy development, legal review, and training. Moreover, Ofcom's assumption that these systems can be applied uniformly across all user-to-user services overlooks key operational differences. In most games environments, sanctions already occur through automated enforcement triggered by verified reports, behavioural flags, or moderation review. Introducing additional layers of record-keeping, appeals processing, and reporting to meet regulatory documentation requirements would significantly increase administrative workloads without necessarily improving user safety outcomes. The costs of compliance are not limited to initial implementation. Ongoing reviews, data storage for enforcement records, and staff time for managing appeals or external audits contribute to cumulative expense. For smaller developers, these ongoing obligations may divert resources from other player safety or accessibility improvements. Ukie recommends that Ofcom explicitly recognise the sector's existing sanctions infrastructure and the low recurrence of illegal or harmful content in video games. The Codes should provide flexibility for services to demonstrate compliance through their existing trust and safety frameworks, rather than requiring entirely new policy infrastructures. A proportionate approach — supported by guidance rather than prescriptive standards — would en-

Question	Your response
	sure that all services can meet regulatory expectations effectively, sustainably, and without undue disruption to their operations or player communities.
Question 41: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie and its members fully support the objective of keeping children safe online but remain concerned that Ofcom's proposed measures on highly effective age assurance (HEAA) risk being overly prescriptive and disproportionate to the level of risk present in most video games environments. The video games industry has a decades-long record of applying age-appropriate design and information standards through established frameworks such as PEGI, which is embedded in UK law under the Video Recordings Act. This system provides clear, pre-contractual information to parents and carers and operates alongside platform-level parental controls that effectively restrict children's access to inappropriate content and features. Age assurance technologies can play a role in certain higher-risk contexts, but Ofcom's proposals in ICU B1, D15, and D16 appear to extend their application far beyond where they are technically necessary or proportionate. Many online games already integrate safety-by-design principles — for example, disabling chat or voice features for under-18s by default or allowing parental approval before online play — which achieve the same child-protection outcomes without requiring intrusive age verification processes. In low-risk, closed or moderated environments, mandating HEAA could create friction for legitimate users, increase compliance costs, and raise privacy and data protection concerns, particularly where biometric or behavioural profiling tools are used. Ukie urges Ofcom to maintain flexibility by focusing on outcomes rather than mandating specific technologies. Services should be allowed to demonstrate compliance through a combination of parental control systems, platform-level protections, and age-appropriate design principles that already exist and have proven effective for decades in protecting children while preserving privacy and accessibility.

Question	Your response
Question 42: Do you agree with our proposal to introduce age assessment appeals measures into the Illegal Content User-to-user Codes (ICU D15 and D16)? Please explain your reasoning.	Ukie supports the principle that users should be able to appeal incorrect age assurance decisions, as this provides an important safeguard for fairness and accuracy. However, the proposal in ICU D15 and D16 needs to be proportionate and practical. For most games services, appeals would require building and maintaining new administrative processes, creating an additional burden for companies that already operate robust customer support and account recovery systems. In many cases, platform-level parental verification systems already allow for age correction or parental overrides, meaning that duplicating these processes at the service level would be unnecessary. Ofcom should clarify that where appeals mechanisms already exist through trusted third-party platforms such as console ecosystems or app stores, these can satisfy regulatory expectations. The focus should remain on ensuring users have access to a fair and accessible correction process, not on mandating parallel systems that replicate existing, effective solutions.
Question 43: Do you agree with our proposed amendments to codify the definition of highly effective age assurance in the Protection of Children User-to-user Code? Please explain your reasoning.	Ukie agrees that clarity and consistency in defining "highly effective age assurance" are important but remains concerned about how Ofcom's codification will be interpreted in practice. Any definition must remain flexible enough to account for a wide range of service models and technological approaches. Current HEAA tools vary significantly in their accuracy, privacy safeguards, and accessibility. Overly narrow definitions could inadvertently privilege a small set of commercial providers, creating barriers for innovation and competition while limiting companies' ability to deploy contextually appropriate solutions. The definition should recognise a layered approach to child safety, combining parental involvement, platform-level controls, age ratings, and contextual design, rather than assuming that technical verification alone constitutes "highly effective" assurance. The video games sector's existing PEGI and parental control systems already meet the spirit of this requirement without the privacy trade-offs that some newer HEAA technologies entail.

Question	Your response
	Codification should therefore reflect proportionality, privacy preservation, and flexibility in implementation.
Question 44: Do you agree with our proposed amendments to the Part 3 Highly Effective Age Assurance Guidance? Please explain your reasoning.	Ukie believes that Ofcom's proposed amendments should place greater emphasis on proportionality, privacy, and practical feasibility. The current draft guidance appears to conflate "effectiveness" with technological intensity, assuming that more data collection or intrusive verification methods necessarily deliver better outcomes. In reality, user safety depends not only on accurate age estimation but also on the responsible design of services, transparent communication, and user empowerment. The guidance should explicitly recognise that the risk associated with user interaction varies widely across sectors. For example, online games often involve limited, gameplay-focused communication rather than open-ended social networking. In these environments, existing protective measures, including pre-screened interactions, parental controls, and account-based restrictions, are already delivering strong safety outcomes. Mandating HEAA on top of these systems risks introducing duplication and unnecessary complexity, especially for SMEs that lack the resources of larger platforms. Ukie recommends that the guidance focus on outcome-based principles and include an explicit exemption pathway for services that can demonstrate equivalent or greater safety outcomes through alternative measures.
Question 45: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie does not agree that Ofcom's cost assessment adequately reflects the financial and technical implications of implementing HEAA at scale. The costs of integrating, testing, and maintaining compliant age assurance systems are significant, especially when multiple jurisdictions have different definitions or standards for effectiveness. For small and medium-sized developers, these costs could be prohibitive and may deter investment in online features or cross-platform integration. Implementing HEAA would also require extensive user experience redesigns, privacy impact assessments, and ongoing compliance monitoring. Many existing systems,

Question	Your response
	such as PEGI-linked parental controls and console-level verification, already deliver effective age gating without additional cost or data processing burdens. Requiring each individual service to duplicate these systems risks fragmenting the user experience and undermining the interoperability that makes age assurance effective in the first place. Ukie therefore recommends that Ofcom adopt a proportionate and risk-based approach, recognising existing industry frameworks as compliant where they achieve equivalent outcomes. This would avoid unnecessary duplication, reduce costs for SMEs, and preserve the UK's reputation as a balanced and innovation-friendly regulatory environment.
Question 46: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	NA
Question 47: Do you agree with option A and option B in increasing the effectiveness of the ICU F1 and F2 measures?	Ukie welcomes the inclusion of two implementation options, as this provides flexibility for services to determine which approach is most appropriate. However, we believe Option B — applying safety settings and supportive messaging to all users — is likely to be both more practical and privacy-friendly for many services, particularly those already operating in low-risk environments or where child-specific verification is not feasible. Option A, which relies on highly effective age assurance, may introduce unnecessary friction and data processing for both children and adults. Given ongoing concerns around the technical maturity, cost, and intrusiveness of HEAA systems, many services may find that applying protective settings universally is simpler, safer, and equally effective. For example, in-game communication tools are already heavily moderated and restricted. Extending supportive messaging and privacy defaults to all players — rather than trying to distinguish between adult and child users — can enhance overall community safety while avoiding complex data collection or verification processes. This approach aligns with the sector's existing safety-by-design

Question	Your response
	ethos and avoids inadvertently excluding legitimate users due to false age assessments. Ukie therefore recommends that Ofcom explicitly confirm that both options are valid and that services should have full discretion to determine which approach best fits their risk profile, existing safeguards, and operational capabilities.
Question 48: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	Ukie does not agree that Ofcom's impact assessment sufficiently reflects the operational and financial implications of integrating highly effective age assurance into live services. Implementing HEAA across large-scale or multi-platform games would require significant technical re-engineering, including identity management integration, user interface redesign, and new privacy and data protection frameworks. For many companies, particularly SMEs, this would represent a disproportionate cost given the low risk of grooming or similar harms within their platforms. Applying Option B (protective defaults for all users) would generally be less costly, simpler to deploy, and more consistent with existing moderation frameworks. Many services already provide privacy and reporting features universally, not only for children. The industry has also demonstrated that user education and parental tools, rather than age verification, are often the most effective means of promoting safe play. Ofcom's cost estimates should therefore differentiate between sectors and risk levels. Imposing HEAA as a de facto requirement could stifle innovation and increase compliance burdens without producing commensurate safety gains. A risk-based approach — recognising the effectiveness of existing child safety systems in the video games sector — would better achieve Ofcom's objectives while maintaining the stability and competitiveness of the UK's creative industries.

Question	Your response
Question 49: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	NA
Question 50: Do you agree with our proposed definition of 'crisis'? Please explain your reasoning, and if possible, provide supporting evidence.	NA
Question 51: Do you consider these measures to be effective for services that are not large services? Please provide any evidence on the role of services that are not large services during crises.	NA
Question 52: Is there any evidence of best practice in responding to a crisis that we have not identified? Please explain your reasoning, and if possible, provide supporting evidence.	NA
Question 53: Do you agree with our assessment of the impacts (including costs) associated with this proposal? please provide any relevant evidence which supports your position.	NA
Question 54: Do you agree with our proposals? Please provide your reasoning, and if possible, provide supporting evidence.	Ukie supports the principle of ensuring fairness and due process in moderation decisions, particularly where user rights could be affected. Extending appeal rights to include actions taken against "proxies" for illegal or harmful content may provide additional safeguards, but Ofcom must ensure that these requirements remain proportionate and practical for services of different sizes and operational models. In many cases, games companies already provide clear appeal mechanisms through their customer support systems, often integrated with console or platform-level moderation tools. These systems enable users to contest moderation decisions related to in-game content, com-

Question	Your response
	munication, or account enforcement. Extending the appeals requirement to cover "proxies" could risk introducing administrative burdens that go beyond what is operationally necessary, especially where moderation decisions are based on clear breaches of community standards or automated detection of known harmful patterns. The concept of "proxies" for illegal or harmful content also needs clearer definition to avoid overextension. For example, terms or symbols associated with illegal activity may appear in benign contexts, such as user-generated content used for parody or education. Requiring appeals in all such cases could lead to excessive workloads and slower enforcement against genuinely harmful content. Ukie therefore recommends that Ofcom's guidance clarify that the extended appeals requirement applies only where there is genuine uncertainty or discretion in the moderation decision, and that services can satisfy the requirement through existing customer service and moderation workflows rather than creating standalone systems.
Question 55: Do you agree with our assessment of the impacts (including costs) associated with this proposal? Please provide any relevant evidence which supports your position.	Ukie does not agree that Ofcom's assessment fully captures the operational and financial implications of broadening the scope of appeal mechanisms. Implementing additional appeal processes, training moderators on new categories of content, and maintaining detailed audit trails would require additional staffing and infrastructure investment. For large services, this would mean scaling moderation review teams and developing new tools to log and review appeals specific to "proxy" determinations. For smaller developers or publishers, the same requirements would represent a significant fixed cost that cannot easily be absorbed. Existing moderation and reporting systems in the games sector already include escalation routes for contested actions, and many companies operate transparent review processes that satisfy both user expectations and legal standards. Imposing additional, prescriptive appeal measures could divert resources away from proactive safety work—such as user education, automated detection improvements, and community moderation tools—that have proven more effective at reducing harm.

Question	Your response
	Ukie recommends that Ofcom adopt a proportionate approach by recognising existing, equivalent appeal systems as compliant; allowing flexibility in how appeals are logged and reviewed, depending on the service's size and risk profile; and providing a realistic implementation period (at least six months) for services to integrate new processes. A risk-based and pragmatic approach will ensure that the intended human rights protections are achieved without imposing disproportionate administrative costs or slowing the responsiveness of moderation systems.
Question 56: Do you think our package of proposed measures is proportionate for services in scope of the Illegal Content User-to-User Codes, taking into account the existing package of measures, the impact on reducing the risk of relevant harms and the implications on different kinds of services?	Ukie does not believe the full package of measures proposed in this consultation can be considered proportionate, particularly when viewed in combination with the already extensive requirements of the existing Illegal Content and Protection of Children Codes of Practice. The cumulative effect of new obligations—covering livestreaming, proactive technology, hash matching, crisis response, user sanctions, and highly effective age assurance—creates an unstable and constantly shifting regulatory environment. The repeated layering of new requirements before previous codes have been implemented or evaluated risks undermining both compliance and innovation. For video games companies, many of which operate multiple services under a single corporate structure, the burden of reassessing risks and updating technical systems for each new set of amendments is significant. Ofcom's previous three-month implementation periods have already proven unworkable, forcing companies to divert resources from user experience and product development towards repeated rounds of compliance. Moreover, many of the proposed measures are prescriptive rather than outcome-based. This limits the flexibility for services to use existing, effective approaches—such as PEGI age ratings, platform-level parental controls, and contextual moderation systems—which already deliver high levels of safety within games environments. The proposed "package" also fails to adequately distinguish be-

Question	Your response
	tween high-risk, open social media platforms and structured, low-risk interactive entertainment environments such as online video games. Ukie urges Ofcom to pause the introduction of new obligations until the first set of Codes has had at least twelve months of full implementation and evaluation. Proportionality should be assessed not only in terms of risk reduction but also in terms of operational feasibility, cost impact, and the need for regulatory stability that allows creative and technical innovation to continue in the UK's world-leading games sector.
Question 57: Do you think our package of proposed measures is proportionate for services in scope of the Protection of Children User-to-User Code, taking into account the existing package of measures, the impact on reducing the risk of relevant harms and the implications on different kinds of services?	Ukie strongly supports the goal of protecting children online but maintains that Ofcom's current approach risks over-regulation and duplication. The Protection of Children Code already includes extensive safeguards, including requirements on reporting functions, moderation standards, and proportionate child safety features. The new proposals—particularly those mandating highly effective age assurance, additional proactive technology, and expanded moderation—go beyond what is necessary for most services, especially those in low-risk environments such as video games platforms. The UK video games industry already operates under a robust framework of protections. The PEGI age rating system provides clear content guidance to parents and children, and platform-level parental controls allow parents to manage access to online play, spending, and communication. These measures are well understood, consistently applied, and demonstrably effective. Imposing additional obligations without recognising these existing protections risks creating confusion, duplication, and unnecessary costs. Ofcom's cost modelling does not adequately reflect the scale of investment already made by industry to comply with the first Codes of Practice. Requiring new systems before the previous ones have been evaluated will disproportionately affect small and medium-sized developers and service providers, who lack the resources of large international platforms.

Question	Your response
	In Ukie's view, a proportionate approach would involve Ofcom: • Allowing a full evaluation period for the existing Codes before layering on additional measures; • Adopting an outcome-based framework that recognises existing, effective safety systems as compliant alternatives; and • Providing longer, more realistic implementation periods for any future amendments. Such an approach would achieve meaningful and sustainable improvements to child safety online without undermining the creative and technical innovation that defines the UK's video games industry.
Question 58: In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? Please explain your reasoning and provide supporting evidence where possible.	NA
Question 59: Do you consider that our proposals could have any negative impacts on certain groups? If so, please explain your reasoning.	NA
Question 60: 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? 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	NA

Question	Your response
use Welsh and treating Welsh no less favourably than English.	

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