



Ukie response to the Draft Online Safety Bill Joint Committee

24 September 2021

ukie

ukie.org.uk | hello@ukie.org.uk
@ukie | +44207 5334 0680

Submission from the UK interactive entertainment association (Ukie) to the Draft Online Safety Bill Joint Committee.

Contact: tim@ukie.org.uk, Tim Scott, Head of Policy and Public Affairs

About Ukie

1. Ukie is the trade body for the UK's games and interactive entertainment industry. A not-for-profit, it represents more than 500 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 games and interactive entertainment industry by optimising the economic, cultural, political, and social environment needed for businesses in our sector to thrive.

About the games industry

2. The UK video games industry is an economic powerhouse as well as a hotbed for the development of emerging technologies, supporting nearly 50,000 FTEs and providing £2.87 billion in gross value add to the UK economy. On top of this, the games industry is 35% more productive than the UK industrial average and is spread across all four nations from Dundee to Belfast, Cardiff to Newcastle.
3. Video games are also a significant part of modern popular culture with broad appeal to a diverse audience, with 86% of people aged 16-69 in the UK having played games in 2020 as well as an even gender split¹. With an estimated 44.32 million video games players in the UK, it comes as no surprise that the UK is the 6th largest market for games in the world, sitting just below China, the United States, Japan, South Korea and Germany. The coronavirus pandemic has demonstrated the value of games more than ever before, as millions of people turned to games to maintain their social connections and keep entertained. It was because of this access to a wide audience that the government worked with the games industry to share public health messaging during the peak of the pandemic.
4. Ukie welcomes the opportunity to submit evidence to the draft Online Safety Bill Pre-Legislative Scrutiny Committee to assist in its assessment of whether the current form of the Bill achieves the government's policy objectives of both making the UK the safest place to be online, as well as supporting the UK's economic growth. Our response is part of our ongoing collaborative engagement with the government on this issue, including our last response to the Online Harms White Paper consultation. We look forward to working with the government and Parliament as this Bill progresses and drawing upon our industry's extensive experience in keeping our online communities safe. This would be in addition to providing our perspective as a

¹ <https://info.savanta.com/uk-gaming-attitudes-and-behaviours>

sector which contributes significantly economically and culturally across the UK².

Summary

5. Our industry is committed to creating safe, fun, fair and inclusive playing experiences for our consumers and has worked hard to create a robust self-regulatory regime that ensures players and parents are provided with transparent information and robust tools and safety features to ensure this remains the case. As a result, we strongly support the aims of the Online Safety Bill. Important measures in the Bill that we appreciate and believe should be maintained include:
 - a. **Focus on user-to-user interaction:** the Bill rightly stays away from other areas of online content already covered by consumer law, intellectual property law, and other regulations. We urge the Committee to retain this focus and not let the scope of the Bill expand further.
 - b. **Proportionality:** the Bill seeks to place the strictest regulatory requirements on those services where users are most likely to encounter illegal or harmful material. We appreciate the acknowledgment that a one-size-fits-all approach would be ineffective and damaging, and welcome the inclusion of categorisation. This approach should be taken further with more clarity on the criteria for categorisation, particularly with an understanding that focus should be aimed at services where illegal content is most likely to be found.
 - c. **Focus on good practice by service providers:** the Bill mostly requires services, particularly those in Category 2, to have effective and well-considered internal processes to ensure user safety, rather than asking the regulator to intervene in individual cases. We believe this to be the correct approach.
 - d. **Ofcom as regulator:** we support the appointment of Ofcom as regulator, as an experienced and effective body with the capability to expand its remit, if given sufficient resources.
6. However, there are aspects of the Bill which are cause for concern. These include:
 - a. **Uncertainty of categorisation:** It is currently not possible to tell which services will fall into Category 1, making it hard to judge the proportionality of the system. There should be a clear focus on not only services with the largest number of users, but those with interaction functions and norms that

² <https://ukie.org.uk/regional-economic-report>

create the largest risks of user interactions involving illegal or harmful content to ensure the Bill is well targeted and, as a result, most effective.

- b. **Excessive penalties:** introducing criminal liability for senior executives of service providers, on top of the proposed significant fines based on global turnover, risks damaging future investment into Britain by global tech firms, including in the games industry.
 - c. **Wide remit of the regulator:** the Bill grants significant room to the regulator and Secretary of State for Digital, Culture, Media and Sport, to set codes and standards, and to determine large parts of how the Bill should operate, including which services it should apply to. This risks creating significant uncertainty for online service providers. To balance this, we would appreciate clearly defined parameters regarding scope and the regulator's remit set out in advance, with appropriate implementation periods for in-scope services to sufficiently prepare.
 - d. **Lack of clarity on fees:** it is not clear from the Bill which service providers will be required to provide funding to Ofcom, nor how much they will have to pay. Again, this risks creating confusion and a chilling effect on future investment.
 - e. **Lack of clarity on age verification requirements:** requiring large parts of the internet to directly age verify users would be disproportionate and a massive risk to the privacy of UK citizens. It has already proven challenging to implement effectively in the regulation of well-defined adult content websites. We support the government's decision to allow service providers to find more proportionate solutions but are concerned that the current wording does not reflect a risk-based approach in this area.
7. Overall, the Bill sets out a relatively reasonable structure, focused on requiring user-to-user service providers to have sensible policies and practices to protect their users. We are confident that the vast majority of games companies to which this regulation will likely apply would already meet the majority of these requirements, thanks to our industry's long-standing record of proactive, collaborative self-regulation. However, much of the detail in the Bill is left open, making it impossible currently to understand exactly what effects it will have, and removing Parliament's ability to scrutinise and assess accordingly. We suggest that this be rebalanced to ensure that the Bill achieves the government's aim of protecting consumers from online harms whilst not disincentivising investment in the UK through the introduction of overly broad and draconian legislation.

The games industry's approach to online safety

8. Our submission is reflective of, and draws from, the games industry's long track record in spearheading self-regulatory efforts. All game platforms and nearly all game publishers have robust terms of use that set expectations for safe and inclusive behavior and which they apply to discipline against disruptive play. This is in addition to technical safeguards such as chat filters, reporting mechanisms, content filters and dedicated moderation teams which work together to make the experience of players one of the safest and most sophisticated online environments. We welcome the opportunity to further share these measures with the committee as an example of how to ensure safe and fun online communities.
9. These measures are in addition to the Pan-European Game Information system (PEGI). Europe's video games sector has undertaken initiatives that go beyond basic compliance with the law and has set pan-European self-regulatory standards protecting children, through PEGI (used today in 38 European countries).
10. The PEGI System is based on a **Code of Conduct** - a set of rules to which every publisher using the PEGI system is contractually committed. The Code deals with age labelling, promotion and marketing and reflects the video games industry's commitment to provide information to the public in a responsible manner.
11. This Code reflects the interactive software industry's commitment and concern both to provide information to the public on the content of interactive software products in a responsible manner and also to ensure safe online gameplay for children. This industry's contribution complements existing national laws, regulations and enforcement mechanisms.
12. It is important to note that the nature of online interaction within games is nuanced – user-to-user communication functions are **often ancillary rather than core to online games services**. They are often a simple text or voice chat option, limited to a specific group of players interacting for a short amount of time. The ability to share video, images or other file-types is rare, as the purpose of the communication is solely to support gameplay.
13. It is important not to confuse in-game communication offered by the publisher or platform hosting the game, with third-party communication platforms that players may use to communicate instead of the functions available in games. These are entirely separate services over which the games companies themselves have no control, and must be regulated as such.
14. In addition, the games industry has for many years actively engaged with law enforcement agencies and Government to protect its players. For instance, the industry has been working closely with the National Crime Agency and NCMEC on how to best protect users from online abuse and CSEA material, as well as the Home

Office and CEOP on how it can communicate effectively on key digital safety topics.

15. Whilst the games sector has led the way in developing technological safety features, parental controls and robust moderating mechanisms to ensure player safety and welfare, the importance of digital literacy cannot be understated.
16. The games industry has always taken a proactive approach to raising awareness and education around parental controls and responsible play. Our approach has overseen a long history of responsible self-regulation which has led to the development of sector leading online safety initiatives. This approach has been strengthened and bolstered during this lockdown period.
17. In 2020, Ukie launched a major campaign, [Get Smart About P.L.A.Y.](#), which we have amplified in response to the current situation. Our campaign provides guidance for parents and caregivers on how to help set parameters around play, and includes advice on effectively utilizing safety controls in order to limit potentially harmful interactions. We have invested additional funding in this period into strategically targeted digital advertising to ensure our safety messaging is reaching more parents and caregivers as the nation spends more time indoors, and online.
18. This campaign exists in addition to the industry funded www.askaboutgames.com resource and parents' guides, operated by the Video Standards Council, another example of how we ensure parents, players and carers are kept informed. AskAboutGames has specifically [developed advice](#) for families on safe online play in lockdown. On top of this, it has also been commissioned by ParentZone to [produce advice](#) on finding suitable games for families, including tips on only accessing age appropriate content which will be released during the Covid-19 period.
19. The industry also launched the [Family Game Database](#) in the early period of lockdown. The database provides information for parents on games suitable for families, whilst also linking back to key tips on activating family controls on devices to limit spending, screen time, online chat, and age-inappropriate content.

Online Safety Bill Draft Legislation

Categorisation of Services

20. We welcome the approach of the Bill to categorise online services, which acknowledges that a one-size-fits-all approach is unsuitable. This is important for the UK games industry, which is home to global publishers, platforms and many development studios including large and medium sized companies and a wealth of small and micro independent businesses. For the games industry in the UK this diversity means that a one-size fits all approach to online safety would be ineffective as well as impractical, and we welcome the indication that proportionality, feasibility, and ability to apply the various codes of practice will be respected.

21. However, the draft Bill does not yet set out the exact threshold conditions for a company being within a certain category. Currently, it states that this will be determined by the number of UK users that a user-to-user service has and the service's functionalities, with the exact threshold to be determined by Ofcom and approved by the Secretary of State. We understand that this is intended to tie the Bill to Parliament, however this makes it impossible for businesses that have user-to-user services available in the UK to work out whether their services will be treated as "category 1" or "category 2b" services and risks allowing thresholds to change according to the government or Secretary of State of the day which may cause significant long-term uncertainty for businesses.
22. In order for the Bill to achieve the government's stated aims of protecting consumers, whilst maintaining the UK as an attractive place for international companies to do business, the Bill should be focused on protecting users where they are most at risk. As such, Category 1 should be for user-to-user services:
 - a. With a very large user base;
 - b. Where user-to-user communication is core to the service;
 - c. With forms of communication allowing for the easy sharing of user generated content, including not only text and voice communication but also image, video and other file sharing;
 - d. And where there is evidence of significant amounts of actual illegal and harmful content being shared.
23. Clear thresholds should be set out in the Bill, allowing Parliament to approve exactly how the strongest requirements will be placed where the greatest risk exists. In doing so, the Bill should also give greater clarity and detail on how assessments against those thresholds will be made. Subjective terms including "material risk", "significant harm" and how a provider may determine if a child and/or adult is of "ordinary sensibilities" should be more clearly explained in the legislation, as opposed to leaving it to the regulator or the Secretary of State, to avoid confusion and uncertainty for service providers wondering how they will be regulated.
24. Within category 2B, a proportionate approach should be taken to the extent of requirements for transparency and risk assessment on different services. For instance, online services with minimal user-to-user interaction should not be expected to bear the same burdens as full social media platforms or other online services where user-to-user interaction is core to the service's offering. Effective support and guidance will also be required to support many of these companies in understanding this novel regulation and the specific burdens it creates.
25. The Bill is also insufficiently clear on the level of fees likely to be levied on service providers to support Ofcom's work as regulator. Again, we urge that proportionality

be applied in focusing demands on those services where the greatest risks pertain, and where the regulator's work will be focused.

Clarity of Duties

26. The Bill introduces duties on providers of the regulated services. Given the complexities of the Bill (including the different categories of potential harm) we are concerned that different duties could introduce conflicting requirements of businesses. One such example of this includes the duty for all in-scope services to respect freedom of expression, whilst also having to protect users from psychological harm and conduct various risk assessments. Clarity on how such cases should be considered, including where the responsibility for resolution lies, would be welcomed by our sector as would an opportunity to consult on the content of such codes of practice.
27. With regards to the new requirement to include information in a regulated online service's terms of service as to how users will be protected from illegal and harmful content, we strongly believe that the obligation should simply be to ensure that regulated services provide this information to consumers but that the Bill be less prescriptive as to how that information is actually provided. Businesses should be given the flexibility to determine how best to present this important information to their users, and it is very unlikely that placing such information in a service's terms of service will be the best way of ensuring consumers are informed of those measures. The government's focus should be on ensuring that consumers are informed, as opposed to specifying how consumers are informed.

Risk Assessments

28. The Bill sets out that service providers must carry out a risk assessment 'before making any significant change to any aspect of the design or operation of a service to which such an assessment is relevant'. Risk assessments must consider 'how the design and operation of the service (including the business model, governance and other systems and processes) may reduce or increase the risk identified.
29. Our industry is built on innovation, with a diverse range of business models and evolving products. Content and business models aside, there are myriad ways in which our products are experienced and delivered across multiple platforms. We understand the importance of assessing the risk of potential online harms, however, we are equally concerned that if a reasonable balance is not struck, then this requirement will be burdensome for the start-ups, Micro and SMEs which make up a significant portion of our sector and for larger publishers who release multiple games each year. In addition to this, we once again emphasise that the actual prevalence of harm on an online service should be taken into account, as opposed to applying requirements on all online services regardless of actual existence of harms.

Age Verification

30. The games sector is passionate about ensuring the welfare and protection of its young players. That is why the industry has in place extensive safety controls for parents and carers to easily use to restrict contact with other users. The industry has also funded a number of digital literacy campaigns on the existence of these controls and how to use them via the Get Smart About P.L.A.Y.
31. We are concerned by the Bill's requirement to assess whether a service is "likely to be accessed by children" and, in particular, its current definition of the "child user condition". As currently drafted, the definition of the "child user condition" makes it clear that even if a business' online service is not targeted at children, and the business is able to show that children do not make up a "significant" proportion of its userbase, the fact that the service may be appealing to a "significant" number of children, is enough to require the online service to implement the Bill's additional safety requirements for services "likely to be accessed by children". This effectively requires businesses to design their services for an audience in respect of which those services were not intended even when children are not a significant proportion of those services' user bases. This goes further than the ICO's own Age Appropriate Design Code and will essentially mean that all services (unless they implement robust age verification to prohibit children from accessing their services – more on this below) are likely to be treated as services that are "likely to be accessed by children". We believe it should be made clearer in the legislation than requirements for age verification or age assurance should be strictly proportionate and based on level of risk.
32. The explanatory notes to the Bill further state that businesses will only be entitled to conclude that their online services are not accessed by children "if there are robust systems and processes, such as effective age verification measures, in place that ensure that children are not normally able to access the service. Age verification refers to the age assurance measures that provide the highest level of confidence about a user's age." This comes very close to imposing an age verification requirement on the services in scope.
33. Ultimately, our industry is committed to protecting young players. We are therefore concerned that this obligation could be interpreted as effectively requiring some level of age verification or assurance from a large number of service providers, without the appropriate democratic debate it would deserve. Greater clarity is needed from government on what systems would be considered appropriate. The Online Safety Bill has been drafted with the specific intention of establishing the UK as a world leader in online legislation.
34. In addition to these concerns, there is also the fact that a robust, trustworthy and implementable age verification system does not yet exist. The inclusion of age

verification and/or assurance in the Bill would be challenging at this stage as online services will be mandated to use age verification technology that is in its infancy, and which carries its own inherent serious privacy risks. The Bill's own Impact Assessment states that it is currently "unclear" what percentage of businesses would need to adopt age assurance measures, or what other system they may employ, as well as the cost of implementing such technology.

35. With this in mind, though we strongly support the need to protect young people online, we **urge the Committee to closely interrogate the exact demands that will be made on online services of all sizes and types to determine the age of their users**. The potential for a significant impact on user's privacy, as well as the ease of digital business in the UK, should be a major concern. This has already been attempted for adult content sites under the Digital Economy Act and proved unworkable, and it is not currently clear what has changed that should make it a feasible policy for a much larger proportion of all online services.

36. As we have previously called for, if this policy goes ahead, there must be specific support to aid compliance, including deploying sector experts where practicable.

Proposals around illegal and legal but harmful content

37. Giving companies a well-defined responsibility to remove content that is illegal and has a clear definition, for example extremism, terrorism, Child Sexual Exploitation and Abuse, and hate crime is an appropriate measure and an area in which our industry works extensively and closely with law enforcement to achieve. As we noted in our White Paper response however, there remain concerns over 'legal but harmful' content where vague definitions risk causing uncertainty and potentially unworkable expectations on business.

38. We support the inclusion of illegal content in the Bill but **ask the Government to define the specific harms in scope** and provide opportunity for industry to **prioritise those harms which are most serious and relevant to their sector** (and therefore allow industry to take the most effective courses of action as opposed to account for all possibilities at once). Again, as above, support should be afforded particularly for SMEs.

39. **For category 1 companies** we note that, with a broad initial list of harmful content and activity in scope of the Bill, ranging from that which is clearly illegal, to others which are more subjective and contextualised, a significant challenge is presented for businesses and the regulator in working out what to do with respect to content at the margins. In addition to this, it will be difficult for providers to determine who is a child and/or adult of "ordinary sensibilities". The current proposal could potentially enable the regulator to limit access to lawful information or content in an opaque and arbitrary manner and leave companies unclear as to what might be permissible. This situation may become more acute for industries like video games

which sits across both the creative/arts and tech sectors. It may therefore be better for the Bill to link the obligation to a more recognised standard, such as “serious or widespread harm and offence against generally accepted moral, social, or cultural standards” as set out in Rule 4.2 of the UK Code of Broadcast Advertising.

40. The concept of ‘legal but harmful content’ is highly subjective and provides challenges for global industries such as ours which serve multiple territories and cultures. Further clarity by providing businesses clear definitions of what constitutes such content would be appreciated.
41. In addition to this, given the subjective nature of the term, online services should be afforded an implementation period to comply.

Codes of Practice

42. These will be drawn up by Ofcom following consultations with various groups including those who have expertise in public health, those who have suffered harm, and those with relevant expertise in equality issues. These codes however can also be modified by the Secretary of State. We look forward to working with Ofcom to ensure the codes which are relevant to our sector are developed with an understanding of the specific context and needs of games companies.
43. We strongly recommend an implementation period is included in the Bill to allow businesses time to fulfil their new obligations, in line with previous regulatory measures such as the Information Commissioner's Office's Age Appropriate Design Code, and the General Data Protection Regulation.

Ofcom as regulator

44. We are strongly supportive of Ofcom as the right regulator for online safety and we look forward to working with them to help them understand our sector. Games and interactive entertainment are an entirely new sector for Ofcom, and it will be important they are afforded sufficient support to fully understand and work with our industry to ensure they are equipped with the knowledge and understanding to effectively regulate this part of the online environment to meet with the government's policy objectives.
45. However, with increasing economic and social policy developments being directed at the digital sector, there is potential for contradictory and unclear messages coming out of numerous Governmental departments and regulatory bodies. Smaller and younger businesses lacking capacity and resource to comply may struggle, stifling innovation and growth whilst larger established companies may be dissuaded from further investment and growth in the UK. We note the establishment of the Digital Regulation Cooperation Forum (DRCF), something we had called for in our response

to the White paper and which is vital to ensure a coherent digital and creative sector policy and regulatory framework.

46. Clarity over power and responsibilities must also be provided. Instances where Parliament, The Secretary of State and the regulators have a range of responsibilities and powers over each other can lead to confusion for business. The Secretary of State has a relatively significant influence on the thresholds, the codes of practice and other aspects of the proposed Online Safety regulation. We ask that the regulator can act independently to maintain integrity and trust.
47. On business disruption measures, our members have emphasised the need for a clear legal basis and process before pursuing these measures. Further information should be provided around what court process entails and the exact requirements of what an access restriction order can cover. The government should look to include this in the Online Safety Bill.

Excessive penalties

48. Finally, we are very concerned about the significant impact that introducing criminal liability for senior executives could have on the attractiveness of the UK as a location for top talent and the best place to start and grow a digital business. Equally, the government should also consider the impact this will have on consumer choice and the delivery of online services to the UK market if senior managers are to be held liable particularly for subjective legal but harmful content shared between users. In fact, the addition of this clause to the Bill may have the opposite effect of its intention and dissuade professionals from taking these positions.
49. We are committed to continuing to collaborate with government in determining practical and implementable solutions to protecting our players, building upon and drawing from the extensive work our industry has already undertaken. Online safety is an issue we take very seriously as an industry and we look forward to working further on ensuring it for our players.