

Question	Your response
We welcome input from industry on the areas listed below. We encourage stakeholders to respond with feedback so that we can ensure that the guidance helps providers and other stakeholders understand:	
A) Ofcom's powers and providers' duties for transparency reporting, as well as Ofcom's approach to implementing the transparency regime. B) Ofcom's approach for determining what information service providers should produce in their transparency reports. C) Ofcom's plans to engage with providers prior to issuing transparency notices, and on what matters, and whether the proposed engagement plan will be sufficient for helping services to comply with their duties. D) Ofcom's plans to use the information in providers' transparency reports in Ofcom's own transparency reports.	Confidential? – N Ukie is the trade body for the UK's video games and interactive entertainment industry. A not-for-profit, it represents more than 600 games businesses of all sizes from start-ups to multinational developers, publishers, and service companies, working across online, mobile, console, PC, esports, virtual reality and augmented reality. Ukie aims to support, grow, and promote member businesses and the wider UK video games and interactive entertainment industry by optimising the economic, cultural, political, and social environment needed for businesses in our sector to thrive. Our response reflects the fact that our industry considers the safety of our player community as paramount. There are over 3.4 billion players globally, and Ofcom's recent Online Nation 2023 survey found that 38% of UK adults and 57% of UK children reported playing games online. The industry is committed to creating a safe, fun, fair and inclusive playing experience for this large and growing audience, and to provide the information and tools necessary to allow parents, carers, and players to customise their own experience and set their own boundaries. It is a business imperative for games companies to provide safe, welcoming places for their customers to play together online. In such a highly competitive global market, players who do not feel safe always have many options for other games to play – often entirely for free. Any game which develops a reputation as unsafe will quickly lose its audience. All companies have clear terms of service and act to remove any content or interaction

	which breaches those terms, including any illegal content. As a result of these priorities, the video games industry has a long track record of spearheading self-regulatory efforts. Our industry has long provided parental controls on all major platforms, implementing the PEGI system of age ratings, as well as funding consumer information campaigns on how to play safely online. As an industry, we take our responsibility to players of all ages seriously. Our commitment is structured around the following pillars: (i) age appropriate pre-contractual information, (ii) safety by design in online environments, (iii) tools to enable players, parents, and caregivers to set the permissions that are appropriate for them or their children, and (iv) enabling consumer redress and efficient and proportionate enforcement. Additionally, the nature of online interaction within games is nuanced and specific and must be considered when setting guidance. Consideration must also be given to the global nature of many of the platforms and services in our sector. Developing regulation that acknowledges the nature of global businesses and is consistent with the expectations or regulations of other countries is essential. Specifically, the communication capabilities in games are usually far more restricted than the capabilities in social media platforms. It is almost always ancillary to the core features of the service. Unlike social media, the purpose of the communication is to enable, enhance or complement the gameplay. Games services are not there to provide open forums for sharing of ideas and long-term conversations about topics outside of the game. The purpose is purely to discuss the gameplay. The communication is often limited in many ways as a result, such as by the amount of text that can be shared, or the number of recipients. In many cases it is not possible to choose recipients, or to find the same recipients again for continued conversation on a later occasion. Interactions are often session-based, with a
--	--

	purpose to collaborate on moment-to-moment gameplay, not to develop long-term conversations about broader topics.
Are there any aspects in the draft guidance where it would be helpful for additional detail or clarity to be provided?	Confidential? – N As we raised in previous consultations, there continues to remain a clear lack on specifying user metrics and the definition of users. It is worth noting also that video games, as a diverse and evolving medium, do not prioritise, promote, or profile content in the same way social media might. We would like to draw attention to the following key points: • User Engagement Metrics: We acknowledge the importance of tracking monthly active users (MAU) as a key metric for regulatory compliance. However, it is crucial to consider that the calculation of MAU can vary significantly based on the criteria used for measurement. Therefore, we emphasise the need for a consistent definition of 'users' to ensure that MAU calculations remain accurate and comparable across different platforms and services. The lack of a standardised definition could result in confusion and misinterpretation of user metrics, potentially affecting regulatory compliance. • Broad Definition of Users: We believe the current definition of users does not consider the unique nature of video games, especially concerning the inclusion of 'passive' or 'unregistered' users. While it is essential to protect individuals who may be indirectly exposed to online harms, it is equally vital to avoid overinflating user numbers with dormant individuals who do not actively engage with a platform and their online functionalities. For

	instance, counting individuals who merely visit a game's home screen or download a game without any substantial interaction may not align with the primary objectives of the Act. Therefore, we recommend a thoughtful and nuanced approach to defining 'users' that takes into account the level of meaningful engagement required to warrant inclusion. Challenges in Tracking User Numbers: The games industry faces unique challenges in accurately tracking user numbers, particularly for free-to-play games where not all players create accounts. Distinguishing between repeat users and distinct individuals becomes complex without accurate tracking mechanisms. An oversimplified tracking approach could result in misleadingly high user counts, which may not accurately represent the level of user engagement or the potential risks associated with a platform. Therefore, we encourage allowing for development of flexible tracking methods that can adapt to the diverse nature of online gaming, accounting for variations in user behaviour and account creation.
Are the suggested engagement activities set out in the draft guidance sufficient for providers to understand their duties and Ofcom's expectations?	Confidential? – Y ✂

Question	Your response
We are also seeking input that will help us understand if there are other matters that Ofcom should consider in our approach to determining the notices, beyond those that we set out in the guidance. The questions below seek input about any additional factors Ofcom should take into account in various stages of the process, including: to inform the content of transparency notices; in determining the format of providers'	

transparency reports; and how the capacity of a provider can be best determined and evidenced.

Are there any other factors that Ofcom might consider in our approach to determining the contents of notices that are not set out in the draft guidance?

Confidential? – N

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

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

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

Is there anything that Ofcom should have regard to (other than the factors discussed in the draft guidance) that may be relevant to the production of provider transparency reports? This might include factors that we should consider when deciding how much

Confidential? – N

As with our previous consultation responses, apart from asking Ofcom to clearly distinguish video games from other online services like social media, our members also call on Ofcom to take a proportionate approach to

time to give providers to publish their transparency reports.	ensure the process is not overly intrusive or burdensome. Additionally, games companies operate across borders and are already complying with the European Union's Digital Services Act (DSA) transparency reporting requirements. Therefore, in order to ensure a greater level of compliance and reduce the regulatory burden, as Ofcom delivers the UK's online safety regime, Ukie recommends aligning Ofcom's online safety transparency reports with the requirements under the DSA.
What are the anticipated dependencies for producing transparency reports including in relation to any internal administrative processes and governance which may affect the timelines for producing reports? What information would be most useful for Ofcom to consider when assessing a provider's "capacity", by which we mean, the financial resources of the provider, and the level of technical expertise which is available to the service provider given its size and financial resources?	Confidential? – N NA
Are there any matters within Schedule 8, Parts 1 and 2 of Act that may pose risks relating to confidentiality or commercial sensitivity as regards service providers, services or service users if published?	NA

Question	Your response
Finally, we are also seeking input into any matter that may be helpful for ensuring Ofcom's transparency reports are useful and accessible.	
Beyond the requirements of the Act, are there any forms of insight that it would be useful for Ofcom to include in our own transparency reports? Why would that information be useful and how could you or a third party use it?	Confidential? – N NA
Do you have any comment on the most useful format(s) of services' transparency reports or Ofcom's transparency reports? How can Ofcom ensure that its own	Confidential? – N NA

transparency reports are accessible? Provide specific evidence, if possible, of which formats are particularly effective for which audiences.	
---	--

Question	Your response
Please provide any other comments you may have.	
General comments	Confidential? – N It is crucial to emphasise the unique dynamics of the interactive entertainment industry and the significant differences it has in comparison to other online platforms, such as social media. Our content adheres to strict age-appropriate standards, and where user interactions are facilitated, they are typically limited and subject to parental controls or age-based restrictions. Moreover, we employ measures to safeguard player privacy, ensuring that gameplay data is collected and stored anonymously, with no direct link to individual players' identities. We've long advocated for the use of pseudonymised data to protect the privacy of underage users, in line with GDPR regulations that mandate minimal data collection and limited visibility of personal information among users. In promoting responsible gaming, we encourage parental involvement and active choice in setting up parental controls. In addition to high safety and privacy default settings, we believe that parents should be able to make informed decisions about content accessibility and online interactions based on their child's age and maturity level. This approach fosters meaningful parent-child dialogue and oversight of digital activities. Parental consent is paramount in ensuring children's safety online, and our industry has pioneered the development of robust parental control tools across various devices and platforms. These tools empower parents

	to tailor content access, regulate in-game spending, and manage online communication according to their preferences and their child's needs. Through age-branded account types and comprehensive pre-contractual information, we strive to provide transparent and reliable guidance to users and parents. Our adherence to the PEGI system of age ratings, which was established in 2003 and which has had a legal basis in the UK since 2012, underscores our commitment to responsible gaming practices, encompassing objective content evaluation, responsible advertising, consumer redress mechanisms, and stringent privacy standards. Maintaining effective privacy policies and fostering a safe online gaming environment are integral to our industry's ethos, ensuring that users have control over their personal data and avenues for addressing any privacy concerns that may arise. On the issue of privacy, it is worth noting that the data that companies can provide varies due to their own data and privacy requirement. Video game companies vary in the extent to which they have procedures in place to handle the situation of parents seeking to retrieve account information from deceased children. While specific policies may vary between companies, some features of existing policies are. 1. Contact and Verification: Parents or legal guardians usually need to contact the video game company's customer support team to initiate the process. They may be required to provide documentation to verify their identity and relationship to the deceased. What 10 documentation is required, and whether the company is able to confirm identity and relationship to the deceased, depends on the circumstances,
--	--

	including how much information the company gathers and retains for child user accounts. 2. Legal Documentation: In some cases, the company may request legal documentation, such as a death certificate and proof of guardianship or power of attorney, to validate the request. 3. Sensitive Handling: Recognizing the sensitivity of the situation, customer support teams are typically trained to handle such requests in a timely manner and with empathy and discretion. 4. Account Transfer or Closure: Depending on the circumstances and the company's policies, the account may be transferred to the parent or guardian, allowing them to access any remaining digital assets or content associated with the account. Alternatively, the account may be closed upon request, or, in some instances, simply closed by the parent or guardian if they can already access the account via the deceased players' login information and without the need for a death certificate. 5. Data Protection: Video game companies adhere to data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, which govern the handling of personal data, including that of deceased individuals. They take measures to ensure that any actions taken regarding the deceased user's account comply with applicable laws and respect privacy rights. 6. Support Resources: Some companies may provide additional support resources or guidance for families navigating the process of
--	---

	managing a deceased loved one's digital accounts, including how to handle digital assets and online presence.
--	---

Please complete this form in full and return to OS-Transparency@Ofcom.org.uk