Consultation response form

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

Consultation title	Call for Evidence: Statutory reports on age assurance and app stores
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.	Nothing
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	All of the response
For confidential responses, can Ofcom publish a reference to the contents of your response?	Yes

Question	Your response
## Section A – Age Assurance **Question 1**: How have regulated service providers used age assurance for the purpose of compliance with the duties set out in the Act?	Ukie is the trade body for the UK's video games and interactive entertainment industry, representing more than 600 companies from micro studios to major multinational publishers and platforms. The sector generates around £6bn in GVA, employs over 26,620 people directly, and supports around 76,000 jobs across the wider value chain. Games are also mainstream: Ofcom's Online Nation work shows that 57% of UK children and 38% of adults play games online. In such a competitive global market, safety is not just a regulatory requirement but fundamental to retaining players. This is why the industry's approach to the Online Safety Act is anchored in safety and security by design, with age assurance operating as one component of a broader ecosystem that has been intentionally developed over many years to minimise children's exposure to risk. We recognise that Ofcom has raised questions about how certain tools (such as parental controls or age ratings) should be characterised within the broader age-assurance landscape. Rather than relying on any single mechanism, the games ecosystem uses a layered set of signals and design measures that together determine how players, especially younger users, access and experience services. This architecture has been deliberately built over many years and has proven effective because games are professionally created, age-rated works where user-to-user interaction, if present at all, is usually structured, session-based and secondary to gameplay. Safety-by-design therefore remains the primary means by which risks are mitigated, with age assurance functioning as a complementary element that supports age-appropriate defaults and controlled access to higher-risk features. A central component of this system is the age information established at the device and platform-account level. When users create accounts, they provide a date of birth, and where this indicates that a profile belongs to a child or young teenager, it is designated as such and placed within a supervised or family-managed environment with default safeguards applied automatically. Recently, new age-verification flows introduced at the platform level in the UK have significantly increased the reliability of the age signals that flow into app stores and games. These processes involve a one-time verification

Question	Your response
	of the adult account responsible for family management or access to certain communication features, using trusted methods such as identity checks, mobile-network validation, payment-card verification or licensed age-estimation tools. As a result, the age or age-band information shared downstream is now considerably stronger than simple self-declaration. This enhances the ability of stores and services to configure features appropriately, reduces duplication for families, and provides a consistent, privacy-preserving foundation on which regulated services can rely. Classification systems such as PEGI and IARC continue to guide consumers and underpin catalogue management, ensuring that children do not inadvertently access content intended for older audiences through the restrictions automatically applied to child profiles. These systems are not presented as age assurance under the Act, nor do we equate higher age ratings with higher risk; they function as part of a well-established framework that supports informed choices and appropriate access. Where games operate their own account systems, age information is used to shape how online interactions are configured. For younger users, defaults typically restrict open communication, limit public matchmaking, or steer interactions towards safer modes such as friends-only or pre-defined communication tools. For older teenagers, settings are calibrated to allow richer interaction only where appropriate. These design choices speak directly to the duties set out in the Act and demonstrate how regulated services use age-related signals to manage user-to-user features proportionately and effectively. It is important to distinguish between traditional games and services that function more like broader creative or social platforms. Some platform-like environments may adopt more extensive age-assurance steps for particular high-risk features such as voice chat, reflecting their distinct nature. This should not be generalised across the wider games sector, where a very large number of titles have no online communication at all or offer only tightly bound, session-level interaction. In these contexts, the existing combination of platform safeguards, default

Question	Your response
	configurations and established moderation practices already provides proportionate and effective risk management. Age information also informs how providers determine whether the child-user condition is likely to be met. Companies analyse platform age flags, audience research, historic player behaviour, age ratings, support patterns and the intended market for each title. Where providers conclude that a significant number of children are likely to use a service, they apply the relevant child-safety duties across their portfolios. This use of age data has helped structure compliance work and focus attention where it is needed. Taken together, the sector's approach demonstrates that age assurance in games is not an isolated technical process but part of a mature, multi-actor safety system that already operates effectively across platforms, app stores, publishers and families. With strengthened platform-level age-verification processes now being implemented in the UK, this ecosystem is more robust than ever. The statutory report should recognise this integrated model and the leadership the games sector has shown in building and maintaining it.
Question 2: How effective has the use of age assurance been for the purpose of compliance with the duties set out in the Act?	In Ukie's view, age assurance in the games ecosystem has been effective when understood as part of a wider safety-by-design model and not in isolation. It has allowed services to implement age-appropriate defaults, restrict higher-risk features to adults or older teenagers, and support parents in making informed decisions, all of which align with the duties set out in the Act. Crucially, the effectiveness of age assurance in games is closely linked to the sector's distinctive risk profile and to the fact that games are accessed through platform and app-store environments that already incorporate age ratings and parental controls and are increasingly incorporating age assurance mechanisms. There are several strands of evidence that support this assessment. First, comparative harm data shows that games present significantly lower reported exposure to online harms than social media. Jigsaw research has found that while a clear majority of adults and 12–15

Question	Your response
	year olds report experiencing potential online harms on social media, the equivalent figures for games are much lower, in the low single digits for adults and low teens for children. Similarly, data from the US National Center for Missing & Exploited Children's CyberTipline for 2022 indicates that, of around 32 million global reports of child sexual abuse material, only around 8,200 related to video game platforms, which is a tiny fraction of the total. These figures do not prove that age assurance alone is responsible, but they are consistent with a picture in which age assurance, combined with constrained interaction models and strong moderation, is contributing to good safety outcomes. Second, there is evidence that when platform-level age assurance and parental controls are configured and used, they work well. Surveys associated with initiatives such as Ask About Games and Get Smart About P.L.A.Y. show that a high proportion of parents who use game-device parental controls feel they offer the right level of assurance that their children are safe in-game, with most focusing on managing spending, content access and play time. A large majority of these parents report that setting up controls was straightforward, and many say that these tools support constructive conversations with their children about healthy play. This suggests that the combination of age assurance (through age-flagged child accounts) and accessible parental settings is not only technically effective but also socially and educationally valuable. In terms of compliance with the Act, age assurance has also been effective in helping services understand whether they fall within the child-safety regime and in calibrating their responses. The ability to analyse user bases, age ratings, target audiences, market research, and platform flags has allowed companies to identify services that clearly attract significant numbers of children and to apply the child duties accordingly. A further point that merits emphasis is the significance of the statutory exception for services that prohibit certain harmful content in their terms of service and enforce those rules consistently for all users. This exception is important because it reflects Ofcom's implicit recognition of the games industry's longstanding and effective approach to safety. For decades, games companies have

Question	Your response
	operated robust terms of service, clear community standards and well-established moderation practices that are designed to prevent the types of harms the Act is concerned with. The inclusion of this exemption in the final Code of Practice acknowledges that these practices already function as an effective safeguard and demonstrates why additional, intrusive forms of age assurance at the individual game level are generally unnecessary. When combined with strengthened platform-led age assurance, established age-rating systems and carefully designed interaction models, this longstanding industry framework already mitigates risks to children effectively. Ukie's members believe that, in the games sector, age assurance is working reasonably well as a component of a broader system. It helps to segment users into age bands, to restrict certain features to adults or older teenagers, and to give parents confidence and tools to shape their children's experiences. It is most effective when it is combined with robust classification, platform-level parental controls, constrained communication features and active moderation, and when responsibility is shared between device manufacturers, platform stores, games companies and families. The statutory report should acknowledge this integrated picture, rather than treating age assurance as an isolated technical fix.
Question 3: Has user privacy, cost, or any other factor prevented or hindered the effective use of age assurance, or a particular kind of age assurance, for that purpose?	Yes. While games companies support proportionate age assurance and already make extensive use of it through platform systems, ratings and publisher flows, there are clear privacy, cost, technical and ecosystem factors that limit the feasibility and desirability of certain forms of age assurance, particularly highly intrusive or duplicative HEAA solutions. These constraints are especially acute for the small and micro studios that dominate the UK games landscape, many of which create globally successful titles without the resources of large social media companies, and studios that operate free-to-play games where user access friction can directly impact the commercial viability of those games. From a privacy perspective, the games sector has long sought to minimise the collection and processing of directly identifiable personal data, especially about children. Many services operate pseudonymous accounts at

Question	Your response
	the game level, with technical and organisational measures in place to prevent easy linkage between gameplay data and platform identity information. This is a deliberate design choice to reduce risk in the event of a breach and to respect players' privacy. HEAA technologies that rely on document scanning, biometric analysis or intensive profiling can run counter to this approach, because they require players to provide highly sensitive information. Parents are understandably cautious about sharing biometric data or identity documents for their children with multiple commercial entities, and there is a risk that the perceived intrusiveness of these methods could deter engagement with regulated services, particularly those that do not charge players any upfront cost and where the incentive to complete various onerous age assurance processes may not exist, pushing some users towards less regulated environments. Cost and technical capacity are equally significant barriers, particularly for SMEs in the games industry which makes up over 95% of the whole UK games ecosystem. Implementing HEAA is not a simple plug-and-play exercise. It involves integrating third-party tools into account creation and consent flows, adapting user interfaces, conducting detailed data protection impact assessments, and building new back-end systems for logging, appeals and error handling, all of which comes at a cost. For cross-platform games running on console, PC and mobile, the same integration work must often be repeated or adapted several times to meet the requirements and certification processes of different ecosystems. For a 10–20 person studio, or for a small mobile developer relying heavily on standard platform tools, this level of complexity and expense may be unmanageable, particularly if historical and projected harms on their services are already very low. Similarly, third party age assurance providers will typically charge a fee for each age assurance flow that is completed (even if the player exists the flow without successfully completing the check). The structure of the ecosystem itself introduces further constraints. Many games, especially on console and mobile, do not control the primary account relationship or the app-store infrastructure. It is at that level that age is first collected and that child and family profiles are cre-

Question	Your response
	ated. If individual games are then expected to implement their own separate HEAA, not only would this be a terrible and duplicative user experience, but there is also a real risk of user confusion and churn as well as a heightened privacy risk. A parent may be asked to prove their identity or their child's age several times for different services on the same device, leading to frustration and reduced trust. From a technical perspective, it is also more efficient and secure for robust age assurance to be handled once at platform level, with games receiving privacy-respecting age or age-band tokens, than for numerous different implementations to proliferate. Ofcom must continue to avoid the temptation of imposing HEAA requirements on all services regardless of risk if the UK's digital economy is to thrive. Regulatory uncertainty has also hindered investment in specific kinds of age assurance. Ofcom's codes of practice have gone through multiple iterations in a relatively short period, and the concept of "highly effective age assurance" has evolved in parallel with technology. Many Ukie members have already carried out two or more rounds of risk assessments and system changes to reflect changes to Ofcom's codes of practice and guidance. Introducing additional, open-ended expectations around HEAA before these earlier measures have had time to bed in creates a moving target that is extremely difficult to design against. While we understand the need to update regulatory guidance as technology evolves, companies will understandably be reluctant to invest in costly HEAA implementations if they cannot be confident that these will still meet Ofcom's expectations in two years' time. This can have the unintended consequence of delaying or fragmenting adoption. Finally, there are important trade-offs between age assurance and other safety objectives. Games derive much of their safety from constrained interaction, strong community management and clear codes of conduct enforced consistently for all users, regardless of age. Many services explicitly prohibit primary priority harmful content in their terms of service and act quickly to remove it wherever it appears. In such contexts, the marginal safety benefits of adding intrusive HEAA for every user may be small, while the impacts on user privacy, cost and service design are large. Ukie members are seeking

Question	Your response
	greater clarity and worked examples from Ofcom on how the statutory exception in the Act, which allows providers to avoid age verification where they explicitly prohibit certain content and enforce that prohibition for all users, will be interpreted in practice. Clear guidance here would enable companies to focus their resources on the combination of age assurance, safety by design and moderation that offers the greatest overall benefit, rather than feeling compelled to adopt particular technologies that may be disproportionate to their risk profile. Ukie's overarching message is that privacy, cost, technical feasibility, ecosystem structure and regulatory stability are all legitimate constraints on certain forms of age assurance. They have not prevented the sector from adopting a layered, shared-responsibility model that is already delivering strong safety outcomes, but they do limit the viability of more intrusive or duplicative HEAA approaches. The statutory report should recognise these constraints and support approaches that embed robust, proportionate age assurance at platform level, provide interoperable age signals to games, and allow services to use a combination of measures, rather than mandating a single, one-size-fits-all solution.
## Section B – App Stores **Question 1:** What role do app stores play in children encountering: a) user-to-user content that is harmful to children; b) search content that is harmful to children; or c) regulated pornographic content **In answering this question, please provide any rationale and evidence where available. To help inform your response, you may wish to consider the role the following categories play in children encountering such content, including:**	From the perspective of the UK games sector, app stores are a key part of the distribution chain and an important safety layer, but they are only one element of a wider, shared-responsibility model. Games are professionally created, age-rated works which are distributed through platforms such as PlayStation, Xbox, Nintendo, Steam, the Epic Games Store, and mobile ecosystems operated by Apple and Google. These platforms run app or games stores that apply their own review processes, age ratings, classification systems and parental controls. Games themselves, in turn, are built on safety-by-design principles and typically offer constrained, session-based communications rather than open-ended social feeds. Against this backdrop, app stores influence which services children can discover and install and how those services are presented, but the actual experience of content and interaction is shaped by the combined actions of platforms, games providers, parents and players as well

Question	Your response
• App review and approval process • App store age ratings • Design and functionality of the app store for child accounts/devices (e.g., discovery and navigation) • Safeguards to protect children from harmful content (e.g., parental controls, setting and enforcement of terms of service).	as the type of game being played and the user-to-user functionality incorporated therein. In relation to user-to-user content that is harmful to children, app stores play a filtering and signalling role through their review processes, age ratings and catalogue design. Console and PC games storefronts are curated environments: before a game can be listed, it is reviewed against platform policies, including expectations around safety and the presence of online features. Age ratings from systems such as PEGI and IARC, which are well-established in the games sector, are attached to each title and displayed on store pages. These ratings include descriptors indicating online play or user interactions. In practice, this means that games which include user-to-user communications are clearly labelled and can be treated differently for child profiles. Platform-level parental controls then allow adults to set limits on what their children can download and which features they can access. Combined with in-game tools such as muting, blocking and reporting, and with AI-supported moderation in higher-risk titles, this produces a layered, multi-actor protection model that is distinct from the dynamics of open social media platforms. For general-purpose mobile app stores, the picture is more varied because catalogues include a much wider range of services, including high-risk social and content-sharing apps. Here, app review and approval processes, combined with app-store age ratings and child-account design, determine whether such services are visible to children at all. Where a child uses a supervised profile with content restrictions, the app store can prevent them from seeing or installing services with higher age ratings or whose core purpose is broad, persistent user-generated communication. However, if a child uses a shared adult account or parental controls are not configured, those same app-store search and discovery mechanisms may surface apps where user-to-user content is more prevalent. In that sense, app stores can either mitigate or facilitate exposure depending on how accounts are set up and how responsibilities are shared and exercised. With regard to search content that is harmful to children, app-store search functions typically return apps rather than web pages or in-app results. The risk they carry

Question	Your response
	is therefore indirect but important: by enabling the discovery and installation of browsers, social networks and media platforms, app stores open pathways to external search environments where harmful content may be more easily encountered. In games-specific storefronts, where catalogues consist mainly of games and related content, this risk is limited; players searching in those environments will primarily see age-rated titles whose content has been reviewed and classified. In general-purpose mobile stores, a child account configured correctly should not be able to install general-purpose apps that expose them to unfiltered search without some form of parental approval. Again, where those account-level safeguards are bypassed, the app store can become part of the route through which children access harmful search content. As to regulated pornographic content, mainstream games storefronts do not normally list dedicated pornographic services, and platform policies prohibit explicit pornography in games. While some games contain mature themes, they are clearly age-rated and are not designed as pornography services. Exposure to regulated pornographic content via console and PC games stores is therefore rare, particularly when child accounts and parental controls are properly configured. On mobile, some app stores host adult-oriented apps in categories such as dating or chat. These are typically age-rated for adults and may be placed behind additional age filters. When child profiles and content restrictions are correctly set up, these apps should not appear in discovery journeys for younger users. Where they are not, the app store may inadvertently facilitate exposure by making such services searchable and easy to install on shared devices. Our members request that Ofcom must explore and understand the role of app stores in the context of games' unique characteristics and the layered safety approach in which platforms, app stores, games companies and families share responsibility. In games, the majority of play does not involve user-to-user communication at all, and where it does, communication is typically short, context-specific, heavily moderated, and session based. Independent evidence shows significantly lower reported harms in games compared with social media, and a tiny fraction of the most serious incidents such as child sexual

Question	Your response
	abuse material originate from games platforms. App stores contribute to these outcomes through review, classification, age-aware catalogue design and parental tools, but they are only part of a system that also depends on in-game design choices and on informed use by families. The statutory report should avoid assuming that the role of app stores in games is identical to their role in open social networks, and should instead recognise the distinct, layered nature of the games ecosystem.
Question 2: To what extent do app store providers currently use age assurance? **Please describe any age assurance methods applied at the app store level (e.g. during account creation, purchase approval, or app/content access), including the purpose(s) for which they are used.** • Where relevant, explain how age assurance applied at the device or operating system level interacts with app store mechanisms. • Where possible, provide evidence or examples of how effective these current processes are in ensuring children cannot access harmful content.	Recent developments at the platform and device-ecosystem level have significantly strengthened the age-assurance processes that app stores rely upon. New age-verification flows are being introduced across major device and platform environments in the UK, requiring a one-off verification step for adult accounts that manage family settings or access full communication features. These verification processes use trusted methods such as secure ID checks, mobile-network validation, payment-card verification or licensed age-estimation tools. As a result, the age information attached to platform accounts is becoming far more reliable than simple self-declaration. This means that when app stores receive an age or age-band signal, it is increasingly grounded in a verified process undertaken upstream. These stronger signals substantially enhance the effectiveness of catalogue filtering, parental-approval flows, purchase gating and access restrictions, providing app stores with a much more robust basis for ensuring that children cannot access harmful or unsuitable content. In practical terms, age assurance at app-store level operates across several points. First, it informs discovery: a child profile signed in to a console or mobile ecosystem will typically see a version of the store catalogue that hides or de-prioritises apps and games above a certain age rating. Secondly, it controls access: attempts by child accounts to download older-rated content can be blocked outright or routed into approval flows where an adult must confirm the action, often using a PIN, password or prompt on their own device. Thirdly, it affects feature availability: in some cases, apps and games can query the platform to determine whether a user is a

Question	Your response
	child or adult profile and adapt their own in-game feature permissions accordingly, for example by disabling voice chat or restricting friend requests for younger users. These platform-level age assurance systems are reinforced by further checks for adult guardian accounts, even if these are not always marketed as "age verification". Payment methods such as credit cards, certain bank accounts and some mobile contracts are generally restricted to adults, and platforms may require additional information or authentication before these can be used for family purchases. This makes it more likely that the person controlling family settings and approving child downloads really is an adult, and that permissions reflect considered decisions. For games companies, this kind of age assurance is extremely important because it provides a shared baseline across platforms and app stores. A child profile on a console carries its age classification into every game on that platform; similarly, a supervised child account on a mobile device brings standardised content and purchase constraints into each app installed from the store. Games that are designed to read and respect these signals can adjust features and defaults accordingly without having to implement their own robust age assurance processes. This supports a layered model in which platform-level age assurance and parental controls sit alongside game-level safety-by-design and moderation, and in which responsibility for keeping children safe is shared. The effectiveness of these processes is positive when used properly. Industry surveys and Ofcom's own research show that an increasing number of parents have set up at least one form of parental control on games devices and mobile platforms, and that those who do so usually find them straightforward and helpful. Many parents focus on limiting spending and content, which aligns well with the way age assurance is integrated into app stores. There is a clear link between correct setup of child accounts and reduced exposure to apps and games that are rated for older consumers. Ukie's position is that app-store providers already use age assurance extensively and that these systems are integral to compliance with the Act in games, but that they

Question	Your response
	cannot and should not be treated as the only line of defence. Their real value lies in providing standardised age signals and parental control frameworks that games can rely on, and in supporting informed choice for families. The statutory report should therefore emphasise strengthening and standardising these existing mechanisms, improving interoperability and parental uptake, rather than expecting every game, including those with minimal or no communication features, to duplicate age assurance tools that are best handled at platform level.
Question 3: What other protective measures and policies currently exist at the app store level to protect children? How effective do you consider they are?	Confidential? – Y / N App stores and platform storefronts operate a range of complementary protective measures beyond age assurance, and in the games context these measures sit on top of, and interact with, the sector's own safety-by-design practices. Games are not open social networks; they are age-rated products whose content has been professionally created and reviewed, and whose online features are layered onto this foundation. The Online Safety Act is therefore entering an ecosystem that already has long-established norms around classification, parental empowerment and moderation. One major component is content standards and app review. Platform holders publish detailed guidelines that prohibit or restrict illegal and harmful material and that set expectations around user safety. Developers, including games studios, must comply with these rules as a condition of listing. Store teams review apps before they are approved and can conduct further checks when updates are submitted. For games, this sits alongside mandatory or widely adopted classification processes such as PEGI and IARC. Games submitted for rating are assessed on factors such as violence, horror, offensive language, sex and online functionality, and receive an age banded rating and content descriptors. App stores display these ratings prominently on product pages and, on many platforms, integrate them directly into parental control systems so that games above a chosen rating cannot be downloaded or played by child accounts. Another protective measure is the provision of child- or family-specific modes and curated views of the store. On

Question	Your response
	consoles, child profiles see home screens and store sections tailored to younger audiences, with featured titles drawn from age-appropriate, family-friendly games. On mobile, many app stores have “kids” or “family” sections where apps are subject to additional review criteria, including stricter rules on advertising, data collection and external links. These curated experiences reduce the chance that young children will encounter borderline or adult-themed titles during ordinary browsing and support parents in finding suitable content quickly. Parental control systems, accessible via app stores and device settings, provide a further layer of protection. These tools allow adults to limit screen time, cap or disable spending, restrict communication features, and require approval for new app or game installations. In games, parental tools can be used to confine communication to pre-approved friends, to disable voice chat or text chat entirely, or to ensure that children cannot join public match-making pools without supervision. Industry-backed education campaigns have helped many parents understand and use these features effectively. Survey evidence suggests that most parents who engage with these systems feel they offer appropriate assurance and find them easy to set up, with many focusing on spending limits and age-appropriate content. App stores also support child safety through enforcement mechanisms. When apps are found to breach content policies or child-safety expectations, platforms can delist them, block updates, or suspend developer accounts. This is a powerful incentive for developers to comply with both legal and self-regulatory standards. In the games sector, this enforcement role complements rather than replaces in-service moderation, but it does provide an important backstop when titles fail to meet expectations. In Ukie’s assessment, these measures are broadly effective for games when they are configured and used by families. They contribute to the relatively low reported harm levels in games compared with social media and help to explain why serious harms such as child sexual abuse material are so rare in games relative to their enormous reach. The main limitations lie not in the absence of protective tools but in gaps in awareness, mis-

Question	Your response
	configuration of accounts, and the sheer scale of general-purpose mobile catalogues, where enforcement must contend with large numbers of apps and diverse business models. Ukie would therefore encourage Ofcom to recognise the existing strengths of app-store protections in the games ecosystem – content review, age-rated catalogues, curated child sections, parental control systems and enforcement – while also highlighting areas where improvements could make these measures more consistently effective. These include more intuitive and prominent parental-control flows, safer defaults for new child profiles, clearer signalling of online interaction features and monetisation in store listings, and greater transparency around enforcement actions against apps that endanger or mislead families. Crucially, any recommendations should be framed within a model that understands safety in games as a shared responsibility between app stores, platforms, developers, parents and players.
Question 4: Do you think that children's online safety would be better protected from the content types listed in Section B, Question 1 by: a) greater use of age assurance; b) particular kinds of age assurance; or c) other measures, at the app store level? **You may wish to consider the categories listed beneath Section B, Question 1 when identifying potential protective measures.** **You may also wish to consider the potential barriers or risks to implementing age assurance, particular kinds of age assurance, or other measures at the app store level.** **Please provide your rationale for your views, and evidence where available.**	Ukie's view is that children's safety would be best served by a balanced combination of particular kinds of age assurance and other measures at app-store level, rather than by a simple increase in the quantity or intrusiveness of age checks. The starting point must be the recognition that games are structurally and functionally different from open social media platforms. The majority of gameplay involves no online communication at all; where online features exist, they are typically short, structured and contextual to matches or sessions; content is professionally created and age-rated; and comparative evidence shows that reported harm levels in games are much lower than on social media. The Online Safety Act is therefore layering onto a mature ecosystem that already incorporates age ratings, parental controls and safety-by-design, and policy should build on that rather than treat all online services as if they were general-purpose social networks. Within that framework, there are contexts in which greater use of age assurance at app-store level may be

Question	Your response
	justified. For example, app categories whose core purpose is adult-only content or unbounded user-to-user communication may legitimately be placed behind more robust, highly effective age assurance, particularly where children have no good reason to use them. However, Ukie does not believe that applying HEAA across the board, including to games with limited or no interaction, would be proportionate. Such an approach would impose significant costs on platforms and developers, including small and micro studios that rely heavily on standard platform tools, without delivering commensurate reductions in risk in a sector that is already comparatively safe. It could also raise privacy concerns and discourage some families from engaging fully (or at all) with regulated services, potentially pushing them towards less regulated alternatives. It would also create a significantly more complex landscape for Ofcom and the ICO to regulate. We therefore favour an approach that prioritises privacy-preserving, interoperable forms of age assurance that fit within the shared-responsibility model already operating across the games ecosystem. A key emerging opportunity in this space is the work of the Open Age Initiative, which is developing open, decentralised age-token frameworks that allow age or age-band signals to be passed across services without revealing personal data. One promising direction is the use of age or age-band tokens generated at platform level following a one-off, robust verification of the adult guardian account. These tokens could then be presented to app stores and games to indicate whether a user should be treated as a child, teen or adult, without requiring individual services to access identity documents, biometrics or other sensitive information. This model would enable games to configure features appropriately while minimising friction for families, preventing duplication across services, and concentrating sensitive information within a very small number of trusted actors rather than dispersing it widely. It reflects the direction of travel in open standards and offers Ofcom a credible, future-proofed way to recognise age assurance that is effective, proportionate and consistent with strong privacy protections. Alongside this, Ukie considers “other measures” at app-store level to be at least as important as age assurance

Question	Your response
	for the kinds of harms Ofcom is concerned with. These include safer defaults for child accounts, such as limiting catalogues to age-appropriate content, disabling or restricting communication features by default, and requiring explicit parental action to relax those settings. They also include clearer, more standardised labelling of online interactions, user-generated content and monetisation in store listings, so that parents can make informed choices quickly; improved, more intuitive parental-control interfaces that encourage correct setup and ongoing use; curated child and family sections that are genuinely quality-controlled; and greater transparency around enforcement actions against apps that undermine child safety. There are real barriers and risks associated with expanding age assurance without regard to context. Large-scale deployment of document-based or biometric HEAA can create significant privacy and data protection concerns. For global platforms, implementing country-specific rules in ways that fit with other legal regimes adds complexity and cost. For small studios and mobile developers, repeated cycles of regulatory change and new technical expectations can be particularly burdensome, especially where guidance is written with the resources and risk profile of very large platforms in mind. If compliance becomes too onerous or inflexible, some developers may respond by removing online features from UK builds or avoiding UK launches altogether, with unintended negative consequences for UK players and the competitiveness of the domestic industry. Ukie therefore urges Ofcom, in its statutory report and subsequent work, to approach app-store responsibilities for children's safety through the lens of proportionality, sectoral distinctiveness and shared responsibility. Games are not open social networks: they are age-rated products, distributed through platforms with their own safeguards, and in many cases they contain little or no online communication. Age assurance at app-store level should be strengthened where it makes a meaningful difference, particularly for high-risk categories, but it should not be treated as a panacea. The greatest benefits will come from a combination of targeted, privacy-respecting age assurance; robust, user-friendly parental controls; clear information and labelling; curated experiences for

Question	Your response
	children; and continued investment by games companies in safety-by-design and effective moderation.

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