

ICO consultation: 'Likely to be accessed' in the context of the Children's code

Age assurance: Adult-only sites likely to be accessed by children

Start date: 24 March 2023

End date: 19 May 2023

INFORMATION COMMISSIONER'S OFFICE INTRODUCTION

In September 2022, we clarified [our position](#) that adult-only services are in scope of the Children's code if they are likely to be accessed by children. To support [Information Society Service providers \(ISS\)](#) to assess whether children are likely to access their service, we have developed the following guidance:

- [FAQs](#)
- [List of factors](#)
- [Case studies](#)

We are seeking your feedback on the supporting guidance documents on 'likely to be accessed' in the context of the Children's code and the accompanying [impact assessment](#).

ICO QUESTIONS:

SECTION 1: FAQs AND LIST OF FACTORS

Q 1.

To what extent do you agree that the FAQs provide helpful guidance for providers of ISS to assess whether children are likely to access their service? If you think that it is not helpful, please explain why specifically and what you think we should change in the comments box.

MGIF Response: Disagree

MGIF Comment: The Mobile Games Intelligence Forum (MGIF) welcomes efforts by the ICO to provide helpful guidance for ISS to assess whether children are likely to access their service. As such, we appreciate the continued engagement with the online games sector, acknowledging that we are but one of a large swathe of ISS that may fall under the scope of the Code.

MGIF has continued to stress that protecting the safety of younger users is of the utmost importance – recognising that children not only need special safeguards and care in all aspects of their life, but also the opportunity to have a full and rewarding online experience that does not impede their rights. As a participatory Forum of mobile games companies with potentially mixed audiences, we were hopeful that this guidance may quell the uncertainty that has persisted since the Code's application in 2021. Although we appreciate the mammoth task of providing clarity on such a far-reaching and novel concept, we feel there are significant limitations that may cause unintended consequences. We will curb the scope of our response to two areas: 1. The definition of 'likely to be accessed', and 2. The risks regarding age-gating.

First, the Forum believes that the definition of 'likely to be accessed' remains unclear, and, in turn, may impact the Code's purpose, for example, by encouraging the unilateral implementation of age gates. Whilst we appreciate the recognition of a risk-based and proportionate application in the Code itself, more objective and tangible information, that goes beyond 'substantive' and 'identifiable', would enable mobile games developers to deliver a full and safe service offering that does not lock children out where this may not be necessary. It is vital that developers are empowered to interpret the Code in the way it is intended, via clear and certain terms that do not inhibit compliance.

Since the inception of the ICO's Children's Code, similar codes have cropped up throughout Europe and the rest of the world. Domestically, the upcoming Online Safety Bill will have its own 'likely to be accessed' threshold. Divergent approaches create an unwanted grey area around compliance which may impede the ability of an ISS to correctly interpret its obligations. Even the recently enacted California Age-Appropriate Design Code, which, as the Forum understands, the ICO heavily influenced, appears to have veered away from the UK's namesake. Respectfully, considering the cost of non-compliance, we have concerns that regulatory

fragmentation may lead to a heavy burden that leads to a service age-gating their product, when they may not need to, out of confusion.

Second, the Forum would like to express concerns relating to the ICO's suggestion that ISS either apply the Code to everyone or implement age verification to ensure that children are unable to access their service. Though we support robust age assurance measures that align to the Code's values of proportionality and risk-based application, this position, in addition to the uncertainty relating to when the Code applies by virtue of a 'significant number of children' accessing a service, may encourage ISS more generally, to apply age gates that lock children out of a rich user experience. Echoing the views [shared](#) by Ireland's Data Protection Commission, 'age verification measures may be perceived by children as blocking them from the more complete 'full' service offering, or as blocking them from accessing other features of the service they are seeking to use' – notably, this concern has 'also been raised by experts in the fields of child rights, child safety and child advocacy'.

Furthermore, although the guidance clearly seems to suggest that all adult directed ISS should implement robust age verification methods, this appears to be based on a desire to prevent all children from accessing these sorts of services as opposed to protecting them from identified high-risk processing. This is not a proportionate approach to data protection regulation and clearly strays into content regulation. The mere fact that some children may access an adult directed ISS should not result in the provider of that ISS having to implement the Code or alternatively robust age verification methods to prevent all children from accessing their ISS.

Instead, the application of the Code must be driven by a reasonable determination of whether a 'significant number of children' are likely to access the ISS. Only then should the ISS provider be required to make a choice between applying the Code or introducing a form of age assurance to prevent children from accessing their service. In each case, the implementation of that choice must remain proportionate to the risks posed by the processing of data collected through their ISS. Further, for those ISS that do involve high-risk data processing, and in respect of which robust age verification may be appropriate, then it is crucial that the ICO provide practical and clear guidance on what such robust age assurance should entail. The alternatives proposed by such guidance must be feasible, appropriate, cost-effective, and secure. Absent such clarity, providers of such services are left grappling with uncertainty.

The guidance, as currently drafted, risks blocking children out from digital services entirely, thus impeding their digital literacy and enjoyment. We do not wish to see a 'walled garden' of limited digital access for children. We ask that the ICO strike the right balance between protecting the safety of children online and serving the educational and developmental needs of children through their access to online services.

Q 2.

To what extent do you think that the list of non-exhaustive factors would be practical for providers of ISS to consider when they are assessing whether children will access their service? If you think that the list of factors is not practical, please explain why specifically and what you think we should change in the comments box.

MGIF Response: Strongly Disagree

MGIF Comment: The current list of non-exhaustive factors suggests that all evidence is created equal and should hold as much weight as other evidence when determining whether or not an ISS is likely to be accessed by children. The list should acknowledge that some factors may be more material than others, such as the existence of any legal requirements to restrict purchases or advertising to consumers above a certain age and the presence of any actual data indicating the overall number of child users on the service.

Less weight should be given to the presence of 'cartoons, animation, music or audio content' in an ISS given how high-level such factors are, or the existence of complaints about children using an ISS if such complaints are isolated or action is taken by the ISS provider to disable the child's access or delete their data as a result of such complaint. Similarly, the guidance should also acknowledge that there may be significant limitations with the quality, credibility, and robustness of third-party research, and caution ISS providers against attributing undue weight to it.

The list would also materially benefit from being separated into factors to consider prior to releasing a new ISS and those that should be considered for existing ISS.

Q 3.

Are there any other considerations that you think should be added to the list of factors? If yes, please explain what factors you think should be included in the comments box below.

MGIF Response: Yes

MGIF comment on following page

MGIF Comment: Our games operate on iOS and Android devices, which have built in controls that can, among other things, limit a child's access to a game and/or its features where they are not the intended audience. When a parent/guardian sets up their dependant's device they should create a child account with the correct age. This facilitates controls, including for example, for under 13s, where spending controls are on by default, and for 13–18-year-olds, where parents/guardians are prompted to implement them. Accordingly, this would protect the rights of the child relating to protection from economic exploitation, as per the remit of the Code. Device-level controls also allow tracking and privacy settings to be restricted.

As such, these controls provide effective and proportionate age assurance, as per the ICO's '[Opinion](#)' at 1.3, where it is referred to as 'approaches used to a) provide assurance that children are unable to access adult, harmful or otherwise inappropriate content when using ISS; and b) estimate or establish the age of a user so that ISS can be tailored to their needs and protections appropriate to their child.'

As iOS/Android devices amount for [98.99%](#) of the mobile operating systems market share in the UK, we believe it is important to include parental controls and controls at the device-level in the list of factors. This would also bring alignment with other European regulators that acknowledge the use of platform-driven parental controls, like the Dutch '[code voor kinderrechten](#)'.

Q 4.

To what extent do you agree that the definition of a 'significant number of children' helps to clarify its meaning? If you think that it is not helpful, please explain why specifically and what you think we should change in the comments box.

MGIF Response: Strongly Disagree

MGIF Comment: We appreciate efforts to provide detail on what constitutes a significant number of children. However, the Forum takes the view that a lack of clarity remains, which may make it difficult to conform to the code and apply a common-sense approach. In particular, defining 'significant' as 'more than a de minimis or insignificant number' is extremely unclear and does not alleviate the problematic subjective element. Defining a concept by using another vague and undefined concept or the opposite of the term you are trying to define is not helpful or clear guidance. Further, if 'significant' is going to be defined as 'more than de minimis' then not only does that appear to be stretching the parameters of what is commonly understood by the term 'significant', but it also makes it virtually impossible for any ISS to appear capable of failing to satisfy that standard.

In addition, importantly, this definition does not consider proportionality. Take, for instance, an ISS provider with a high volume of users, where children account for a minor percentage. Here, it may be reasonable to interpret this as de minimis, as it represents a small proportion of the overall user base. However, with the existing reading not accounting for proportionality, there would be issues with adopting that approach or indeed applying the Code to an audience for whom the ISS was never intended. Objectivity and specificity would enable ISS providers to understand their obligations. A definition of 'significant' that provides objective clarity and proportionality, we feel, would enhance conformance with the code, reduce harms and negate market failure.

SECTION 2: CASE STUDIES

Q 6.

To what extent do you agree that the case studies provide helpful examples of providers of ISS considering whether children are likely to access their service? If you think that the case studies are not helpful, please explain why specifically and what you think we should change in the comments box.

MGIF Response: Disagree

MGIF Comment: MGIF welcomes efforts to provide clarity on this complicated concept of 'likely to be accessed' by developing case studies. We regard protecting the safety of younger users as of the utmost importance – recognising that children need special safeguards and care in all aspects of their life. However, we are concerned that the case study for games does not align with the principles set out in the Children's Code. Therefore, we would be grateful for the opportunity to work with the ICO, to facilitate consistent, clear, and certain regulation.

Content ratings do not reflect data processing or intended audience

We respectfully question why the case study begins by detailing a 'PEGI 18 rated game'. As a content rating, this does not reflect data protection risk. Yet, the case study appears to suggest that a PEGI rating of 18 is an indicator of high-risk data processing, when this is not the case. For example, a video-streaming platform may offer a range of TV programmes and films that range from U (suitable for all) to 18 (suitable only for adults), however this has no bearing on the data processed by the TV set, streaming service, or internet service

provider. MGIF believes it is vital to avoid conflating content and data protection so as not to induce misinterpretation of the law. Ergo, the content rating, whether it is high or low, is not a gauge of data protection risks relevant to the game.

MGIF would also like to take this opportunity to point out that content ratings are not always indicative of the intended audience either. Whilst a higher rated game is likely to indicate an older audience, a game with a lower content age rating is not necessarily designed or intended for, or played by, young audiences. By way of comparison with TV ratings, the popular Channel 4 lifestyle show, 'Location, Location, Location' may be considered suitable for young viewers, though they are not the intended audience.

Conflation of data protection and content regulation may result in the improper delivery of regulation that does not reflect its intention, as was the case in 2021, when it was widely [reported](#) that US lawmakers misinterpreted the ambit of the UK Children's Code, 'making the entire effort extremely confusing'.

Rationale behind the qualifying factors for a 'substantial' number

MGIF respectfully questions the rationale used to determine that a substantial number of children are likely to be accessing the game. In doing so, we would first support a need for evidence-based proportionality when applying the Code.

The case study appears to imply that 'research' showing that parents are less likely to follow age restrictions on video games compared to films is a contributory factor in terms of 'likely to be accessed'. MGIF contends that recent ICO and Ofcom [research](#) shows that parents use a range of methods to oversee children's online behaviours and feel that 'maintaining good communication with their child' about their online behaviours is a high priority over other methods of age assurance.

Parents prefer to give their children opportunities to learn and grow, which may impact their approach to various online activities, and, in turn, the conclusions drawn from this case study. We would appreciate more clarification on the logic behind this implication, as well as information on the type of research used – here, it is important to use a high standard, by, for example, limiting the threshold to scientifically controlled studies.

Moreover, we also respectfully ask for clarification on the case study's use of 'children', 'teens', and 'young people' to contribute to a substantial number of children. Given the conclusions drawn, this may have significant implications for mobile games publishers conforming to the Code. Considering the five age ranges and developmental stages set out by the ICO, a publisher with a game that is intended for adults may face the costly burden of designing several versions for their unintended audience.

MGIF believes that the conclusions drawn from the evidence gathered in the gaming case study may not be proportionate and would appreciate further clarification. One observation is that the actions taken do not seem to be founded upon the type of data being processed, rather a subjective interpretation of research. More information on the relationship between the evidence and the type of data being processed may provide deeper understanding in this case.

An evidence-based and proportionate approach to age assurance

We are concerned that, on age assurance, this case study may presuppose a level of understanding and technological feasibility, which does not currently exist. As such, we request that further information is given on the proportionality of the response.

The Forum appreciates work done by the ICO and collaborators to increase understanding of age assurance. Nonetheless, as a still-emerging area, it stands to reason that there are differing definitions and interpretations – the UK Children's Code itself does not define age assurance. As the recent ICO commissioned [report](#) on age assurance states, age assurance 'techniques are, at present, a nebulous concept with multiple different methods, approaches, measurement challenges and propensity to define. Equally, it is important to recognise that these technologies are constantly evolving and will continue to emerge as further use cases and age-related eligibility challenges are identified'. Furthermore, as the Online Safety Bill progresses through Parliament, the statutory definition of age assurance may evolve.

As a nascent concept, we feel it important to stress the significance of identifying a functional, robust and workable digital identification or age estimation technology that is proportionate to the offering that mobile games provide as well as the unique environment in which they exist. MGIF cannot point to a universal, one size fits all, age assurance solution for mobile games. This is echoed in [Recommendation 7](#) of the French data protection regulator (CNIL) 'recommandations pour renforcer la protection des mineurs en ligne' (2021), which acknowledges that there is no 'miracle solution' to age verification since available technologies are either too intrusive or ineffectual. Recent criticism of the Online Safety Bill's approach to age assurance outlines the pitfalls to premature age assurance. The Forum's commitment to collecting minimal data is paramount to our considerations when protecting children online.

The recent ICO and Ofcom research on age assurance highlights that 'many parents consider not only their child's numerical age, but also their child's maturity and their own perceived risk of the online platform when making decisions about what their children should and should not have access to.' It would be proportionate to acknowledge the role parents play in bringing up their children, as well as their agency in terms of setting boundaries. Parenting in the digital world is a complex area that must be treated with care to ensure

the wellbeing of the family is not compromised.

We welcome any efforts to boost understanding and allay concerns in respect to technical feasibility, accuracy, perspectives of children and parents, economic impacts, data protection risks, fairness, and the avoidance of discrimination and algorithmic bias, especially considering this is an embryonic area of study. Thus, we hope any further setting of tolerances is done with a proportionate and risk-based approach, in consideration of the views of diverse stakeholders.

Mobile games warrant specific considerations

There is a [legal precedent](#) from the United States that mobile games should be considered a distinctive sub-category of video games due to factors such as the freemium pricing model, demographics, growth rate and preponderance of the casual genre. The ICO should, for instance, consider that mobile games are dominated by the casual and hyper-casual genre – where games are quick to learn, easy to play and typically played in short time bursts. Therefore, the friction created by costly age verification systems would be highly inconvenient both for developers to implement and players to navigate. Further, iOS and Android employ user friendly parental controls, such as purchase requests, where a parent receives a notification on their device to approve a purchase - that offer quick and efficient protections to children.

A 2023 Ofcom [report](#) titled, 'Children and Parents: Media Use and Attitudes 2023', shows that girls, who are equally likely as boys to play video games, are more likely to do so on mobiles or tablets – playing casually across several gaming apps. Intrusive age assurance methods may feel inconvenient and deter casual play. Further, the Forum believes there are lessons to learn from the 'information-fatigue' of GDPR pop-ups, that have been [widely reported](#) on.

We would ask that the ICO commits to research on the implementation costs of various age assurance methods specifically for mobile, and the relative efficacy. Citing the aforementioned ICO and Ofcom report, whilst parents and children feel age assurance is appropriate for activities that are more traditionally associated with age restrictions offline, like gambling, watching pornography, buying alcohol, in contrast, parents see minimum age limits on games platforms as not always reflective of what they think is appropriate for their child. As these regulated activities are subject to strict legal requirements including licensing, it is disproportionate and unhelpful to compare the games industry directly with these sectors.

Besides, the resources games companies spend on implementing robust age assurance methods may be in vain. A parent may not want their child's sensitive personal data shared online, particularly with third-party companies they may not know, and so may well be reluctant to share any form of identification as part of an age assurance check.

A common approach and avoidance of cross-regulatory confusion

One of the final elements of the games case study regards the decision to prevent in-game communications to non-logged in users. MGIF believes this may be better suited to the Online Safety Bill and would ask for clarity on how this is a data protection consideration. As with our earlier point on the conflation of content ratings with data protection, the risk of domestic cross-regulatory confusion is real and pressing. Relating to the Online Safety Bill's own approach to 'likely to be accessed' and age assurance, Ofcom will issue codes of practice. We are pleased that the ICO is committed to working alongside them to ensure a coherent approach that clearly distinguishes between considerations of content and data protection.

Finally, as a Forum, we are keenly interested in pan-European developments and support a harmonised approach to regulatory guidance and self-regulation. The Swedish '[Rights of Children](#)' maintains that 'there are no exact rules for how to carry out age checks, but such checks should be preceded by a risk assessment and not entail any unreasonable processing of personal data'. Alternatively, the Dutch '[code voor kinderrechten](#)' aims to be more prescriptive, advising self-declaratory tools in low-risk instances, supplemented by additional measures to discourage and/or detect false age declarations. Meanwhile, the French 'Recommendations' focus on the 'intended audience'. Although there is a divergence of approaches, there are points of commonality that may be seized upon in order to support the shared interest of protecting children's data online.

Q 7 & Q 8.

MGIF chose not to respond to these questions

SECTION 3: IMPACT ASSESSMENT

Impact assessment summary table

We are seeking views on our impact assessment summary table, which was provided as supporting evidence for the consultation. This sets out a high-level overview of the types of impacts that we have considered.

Continued on the next page...

Q 9.

To what extent do you agree that the impact assessment summary table adequately scopes the main affected groups and associated impacts?

MGIF Response: Disagree

MGIF Comment: The Forum would appreciate transparency on the methodology and outcomes of the cost-benefit analysis. For instance, 'familiarisation costs' with additional guidance are estimated to be £13 per affected ISS. We are concerned that it is conceded there are 'significant evidence gaps', yet, on the other hand, it is suggested that the benefits outweigh the costs identified.

Q 10.

Can you provide us with any further evidence for us to consider in our impact assessment.

MGIF Response: No

Impacts on your organisation

These questions are specifically for respondents that are acting on behalf of an organisation.

Q 11.

Who in your organisation needs to read the guidance? (Please provide job titles or roles, not people's names)

MGIF Comment: As Mobile Games Intelligence Forum (MGIF) is an international organisation that represents the mobile games industry and facilitates the sharing of insights and perspectives the CEO, Policy Director, Policy Researcher all need to be very familiar with this guidance in order to try and help interpret and understand it's implementation in the mobile games ecosystem.

Q 12.

To what extent (if at all) do data protection issues affect strategic or business decisions within your organisation?

MGIF Response: Data protection is a major feature in most of our decision making

MGIF Comment: The Forum would appreciate transparency on the methodology and outcomes of the cost-benefit analysis. For instance, 'familiarisation costs' with additional guidance are estimated to be £13 per affected ISS. We are concerned that it is conceded there are 'significant evidence gaps', yet, on the other hand, it is suggested that the benefits outweigh the costs identified.

Q 13.

Do you think the guidance set out in this document presents additional: (select one option)

- cost(s) or burden(s) to your organisation
- benefit(s) to your organisation
- both
- neither
- Unsure/don't know

MGIF Response: cost(s) or burden(s) to your organisation

Q 14.

Could you please describe the types of additional costs or benefits you might incur?

MGIF Response: The costs associated for Mobile Games Intelligence are largely work-hours.

Q 15.

Can you provide an estimate of the costs or benefits you are likely to incur and briefly how you have calculated these?

MGIF Response: MGIF cannot provide costs for itself as a forum and costs will vary for each individual member company.

Q 16.

Please provide any further comments or suggestions you may have about how the guidance might impact your organisation.

MGIF Response: MGIF supports robust measures that align to the Code's values of proportionality and risk-based application, and we believe conformance would vastly improve with clear and certain terms.

SECTION 4: ABOUT YOU

Q 17.

What is your name?

MGIF Response: Luc Delany

Q 18.

If applicable, what is the name of your organisation and your role?

MGIF Response: Mobile Games Intelligence Forum, CEO

Q 19.

Are you acting: (Please select)

- in a private capacity (eg someone providing their views as a member of the public)?
- in a professional capacity?
- on behalf of an organisation?
- other

MGIF Response: on behalf of an organisation?

Q 20.

Are you a: (Please select most appropriate)

- Provider of an Information Society Service. If so please state which sector in the box below (e.g. gaming, pornography, online dating, social media etc)
- Member of the public
- Technology provider
- Representative group/charity/think tank
- Civil society - children's safety
- Civil society - privacy
- Commissioner
- Academic
- Trade body
- Other

MGIF Response: Representative group/charity/think tank

Q 21.

How would you describe your organisation [size]?

MGIF Response: 0 to 9 members of staff

Q 22.

Would you be happy for us to contact you about our work relating to Age Assurance and the Children's Code?

MGIF Response: Yes