Call for evidence response form

Please complete this form in full and return to os-cfe@ofcom.org.uk

Title
Second phase of online safety regulation: Protection of children

Full name
✂

Contact phone number
✂

Representing (select as appropriate)
Organisation

Organisation name
Ukie

Email address
✂

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? (select as appropriate)
Nothing

Your response: Please indicate how much of your response you want to keep confidential (select as appropriate)
None

For confidential responses, can Ofcom publish a reference to the contents of your response? (select as appropriate)
Yes

Your response

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.

Is this a confidential response? (select as appropriate)

No

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.

As an industry, we take our responsibility to players of all ages seriously. We want everyone to be able to enjoy video games in a fun and responsible way. This 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.

Child and user safety is built into the companies' decision-making structures by default and by design. It is a core design principle. All services and software operate within that system and are subject to the same controls.

In addition to the requirements stipulated by law relating to pre-contractual information to consumers, in 2003, the video game industry established the PEGI system which operates through a set of scientifically backed ethical standards in the form of a Code of Conduct. The PEGI system is part of the industry's commitment to protect minors and behave responsibly, especially where children are concerned.

It is important to mention that the interactive entertainment industry varies greatly from other online platforms, including social media. 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. Additionally, the industry collects and stores game play data in a way that does not allow companies to identify the player directly by applying technical and organisational measures to prevent easy linking between the game play dataset and the players' platform account information. The industry has also since long endorsed the use of pseudonymised data as a valid way to protect identity of underaged users.

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

Is this a confidential response? (select as appropriate)

No

Video games are a significant part of modern popular culture with broad appeal to a diverse audience. 86% of people aged 16-69 in the UK have played games in 2020, and this is represented by an even gender split[1]. Ofcom's recent Online Nation 2022 report found that 39% of UK adults and 56% of UK children identify as playing games online[2].

By their nature as one of the most popular forms of entertainment, many games will attract an audience of all ages. Our industry has developed a world-leading rating system that identifies games with content that is inappropriate for younger audiences and a system of parental controls, backed by legal and self-regulatory requirements, to manage that interest from all ages and to provide access to age-appropriate experiences.

Question 3: What information do services have about the age of users on different platforms (including children)?

Is this a confidential response? (select as appropriate)

No

Age is usually obtained through self-declaration only. When children first access a new platform, such as a new console or an online store, they are required to self-declare their age. Even before the GDPR had entered into force, the industry adopted Privacy by Design as a key design principle when new products and systems are being developed.

Game play data, for instance, is usually collected and stored in a way that does not allow companies to identify the player directly by applying technical and organisational measures to prevent easy linking between the game play dataset and the players' platform account information. The industry has also since long endorsed the use of pseudonymised data as a valid way to protect identity of underaged users. The GDPR requires that companies by default should not collect any more personal data than needed for each processing purpose or make users' personal data visible to indefinite numbers of other users.

[1] https://info.savanta.com/uk-gaming-attitudes-and-behaviours

[2] https://www.ofcom.org.uk/__data/assets/pdf_file/0023/238361/online-nation-2022-report.pdf

Question 3: What information do services have about the age of users on different platforms (including children)?

In addition, video game companies often apply technical and organisational measures to prevent linking of the gameplay data with identifiable information. Such anonymised or pseudonymised datasets are safer to handle but still allow to personalise the user experience.

We feel encouraged by the 16 standards of age-appropriate design that have been proposed in the ICO Code as they effectively recognise the work we have been doing so far.

We also agree with Ofcom's recent research that found 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."[3] The research also found that some parents and children raised concerns about sharing their data with online platforms for age assurance, and that parents liked the guardian confirmation as a method of age assurance. As seen in the answer below, this is a method the industry employs in a comprehensive manner as it aims to empower the parents.

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

No

Parental consent is a key concept to ensure that the best interests of the child are considered in a digital environment and that appropriate safeguards are in place. The video games sector is at the vanguard of the development of sophisticated and robust parental control tools on a variety of devices and software applications. These tools, which are made available when setting up consoles, tablets or other handheld media devices that have access to mobile app stores, as well as on the PC stores, allow parents to agree with their children, based on their age and maturity, what type of video game content can be accessed, whether in-game spending will be allowed or limited, or if any data may be shared with others online.

In addition, the parental control systems that are available for free on a variety of devices contain features that allow parents to limit their child's daily play time and to define a "bedtime" after which the child cannot play anymore.

Parents are invited to set up accounts for their children that either limits access to peer-to-peer features or which provide parents with a significant degree of control over their children's online activities, including consenting to the processing of their children's data and

[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0026/245195/DRCF-Ofcom-ICO-age-assurance.pdf

Question 4: How can services ensure that children cannot access a service, or a part of it?

managing with whom and how the child communicates and whether user-generated content may be shared. The different account types are branded by age and determine which content the person can access, as well as providing additional assurance methods.

Our sector generally encourages parents to accompany their children when experiencing videogames and supports the use of active choice. This means that we believe that it is more effective to ask parents to make a series of choices as to the level of parental control and filtering on a device, making them mentally engage with what is appropriate for their family, than to simply have all such controls switched on automatically when they first use the device. An active choice policy strengthens the child-parent interaction and enables the parents to best protect and educate their child.

Additionally, the industry actively encourages its users to report any activity or content they feel uncomfortable or concerned about. Users can easily mute or block players that they come across in games and report inappropriate content/behaviour using the Report Abuse system.

The PEGI system (see answer to question 5) is an important, scientifically backed, system to protect minors by advising parents on the age rating of a game to inform their decision to purchase it for their children. Regardless of the rating, the sector intentionally designs systems to provide a low-risk environment for all users, not just children.

Lastly, the video games sector partners with relevant institutions such as family organisations, media literacy organisations, and public authorities, to ensure that the right audience is reached, and that the information is relevant.

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Is this a confidential response? (select as appropriate)

No

A number of platforms are testing various forms of age verification methods, allowing users to access innovative social capabilities and age-appropriate content while also ensuring the safety of their community. Some companies request an ID document check, followed by a selfie match. They clearly state that the raw ID and selfie data are not stored. Instead, when a government-issued ID is scanned for verification, an anonymized value is generated, allowing the company to safely verify identity without risking exposure of the user's real identity.

Additionally, sophisticated and robust parental control tools are implemented on a variety of devices and software applications that not only allow parents to control access to video

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

game content based on 'their child's age and maturity but also allow them to manage and control how their children access the internet, share their data and interact with others online. Parents can set up accounts for their children providing them with a significant degree of control over their children's online activities, including managing with who and how the child communicates and whether user-generated content can be shared. The parental control tools provided by one industry player have even been officially recognised under the German youth protection regime – it is thus the first youth protection programme for proprietary platforms that has received this level of recognition in Germany, which has been considered a milestone for technical youth protection.

Overall, introducing those stricter age verification technologies both bring significant costs to a business, as well as a less user-friendly experience, leading to the industry preferring reporting mechanisms laid out later in this consultation.

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Is this a confidential response? (select as appropriate)

No

Our members have very little evidence of content that is harmful to children. Their systems are deliberately designed to minimise sharing of and exposure to harmful content, with some platforms carefully restricting user-to-user contact through the sharing of friend codes and limiting groups to small numbers. This is particularly true of games designed for younger audiences, where social interaction is typically carefully controlled to the extent it is allowed at all.

The industry provides various self-assessments on the state of its online chat rooms, analysing and moderating the contents, as well as to act if any harmful content is picked up. It mitigates risk of disruptive content through their tools, including escalation policies for potentially unlawful activity or threats.

The most common form of inappropriate content found in games is disruptive behaviour, such as toxic language or names, as opposed to unlawful behaviour or threats of harm. The industry is committed to tackling such disruptive behaviour, as it reduces the quality of the experience for other users and hence the appeal of the games themselves. However, such work largely falls outside Ofcom's remit.

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

As mentioned above, the industry self-assesses their online services on a regular basis.

However, the sector does not have any evidence of the content creating actual real-world harm.

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Overall, the prevention of harm to children and indeed all users is built into the system by design and by default. Any services delivered are therefore operating within that carefully and closely controlled system which permit only limited user-to-user contact.

The impact assessments, carried out at the design stage to identify and reduce risks, predates the 15 standards set out in the ICO's Age-Appropriate Design Code but reflects similar thinking.

Through methods like age verification, manual interventions into account reclassification and survey-based research, companies can assess factors including on how people access their service, the number of child accounts created, as well as examine reported items of content as a proportion of overall content shared between users.

Note: Due to the short consultation period, Ukie is unable to properly assess the full impact of all age assurance methods used in our sector, nor does the time allow to consider the potential interplay between the draft ICO Code, the Online Safety Bill and other government initiatives related to consumer protection. This is a complex and important area of policy which merits time and care. Ukie, therefore, calls for a continued dialogue with Ofcom that will allow us to gather evidence for an in-depth analysis of each of the proposed standards and to consider all consequences on our sector, including unintentional ones.

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Is this a confidential response? (select as appropriate)

No

The video game industry is aware of the risks related to children in digital environments and understands the importance of establishing practical measure and safeguards.

The sector has undertaken a number of initiatives, which are summarised in the questions below, that go beyond mere compliance with the law and set self-regulatory standards to protect children's privacy, create a safer off- and online environment and promote involvement of parents and carers.

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

Is this a confidential response? (select as appropriate)

No

Child and user safety is built into the companies' decision-making structures by default and by design. It is a core design principle. All services and software operate within that system and are subject to the same controls.

Internal structures and names will vary, but games companies of sufficient size will typically have Online Safety functions or points of contact as part of their Consumer Experience, Product Design, Engineering, Legal and Corporate Communications teams. These teams work cross-functionally on a roadmap of continuous improvement around child user and platform safety and meet regularly to take decisions on the programme's effectiveness in addressing key objectives as well as plan short, medium and long-term future goals. Senior leaders are active participants in these forums.

Companies may also have an ESG (Environment, Social and Governance) function which works across the various stakeholder teams to ensure Online protection is a key corporate goal, has the correct visibility and is adequately supported from a resourcing perspective.

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

Is this a confidential response? (select as appropriate)

No

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

The ICO, through the Children's Code, requires that a child should receive age-appropriate information, including by audio and video, about privacy policies and the functioning of parental controls and that an obvious sign should be displayed when its online activity or location is being monitored.

Our sector has a track record of communicating to parents, guardians and players to promote the use of parental controls whereby we take great care to emphasize that these tools are best utilised by parents and children working together to understand games and game play, rules and boundaries. We have also conducted several public awareness campaigns (see Question 13) to inform parents about on how to set fair rules, and how to start a dialogue and take an interest in their children's online activities.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[4]

Is this a confidential response? (select as appropriate)

No

The terms of service of most of the industry prohibit a wide scope of disruptive content and all unlawful activity, including harmful or offensive content that is vulgar, harassing, abusive, profane, threatening, etc.

The community guidelines must be adhered to and breaching it may result in a user being banned or suspended from a particular game or service.

However, most policy statements do not delineate between "primary" / "primary priority" groups. Instead, current terms / policies focus prohibiting the individual of harms covered in the primary and priority groups. These restrictions apply to all users, irrespective of age. For example, one Ukie member company's Code of Conduct, included in their Terms of Service, states:

- For Primary content:
    - Re self-harm: "Do not threaten, harm, or alarm anyone or encourage anyone else to do so."

[4] See A1.2 to A1.3 of the call for evidence for more information on the indicative list of harms to children.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[4]

- Re pornography: "Do not share material that is pornographic, [or] obscene…"
- Eating disorders is not covered specifically but could be caught in other areas, e.g. prohibition against causing harm to others or against misinformation.

- For Priority content:
  - Re abuse, cyberbullying and harassment: "Do not bully, harass, or stalk anyone." Additionally, the PlayStation Hate Speech Policy also covers content that amounts to online abuse, cyberbullying and harassment.
  - Re violent content: "Do not share material … that depicts extreme or abhorrent violence". However, a case-by-case approach would be beneficial here as many games contain potentially violent content as core gameplay, even for games rated for children. As a result, without clarification guidance from Ofcom, a general ban against any violent content could prohibit sharing any related gameplay.
  - Re harmful health content: this is not explicitly covered but may fall under other provisions against misinformation such as: "Do not share or send information that misleads others."

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Is this a confidential response? (select as appropriate)

No

It is standard practice across the games industry to have reporting functionality easily available within the game, wherever there is interaction with other users, so that breaches of community guidelines can be acted on quickly. There are also commonly features to block or mute specific players or groups. Most games indicate the available reporting methods to the user, in a simple language, when starting the game, as well as through periodic prompts during use.

Ukie also launched the Get Smart About P.L.A.Y campaign[5], encouraging more parents and carers to use tools that manage screen time and in-game purchases on video game consoles.

[5] https://ukie.org.uk/news/get-smart-about-p-l-a-y-children-across-the-uk-to-be-taught-about-responsible-video-game-play-in-the-classroom

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Additionally, Ukie partnered with the VSC Rating Board to create Ask About Games[6], an online tool that teaches parents about age ratings, video games and parental controls, to ensure they get the most out of the games they enjoy together.

In recent research by Media Development UK, researchers found that almost all parents (96%) who claimed their child had been exposed to potentially harmful content took at least one of the abovementioned actions.[7]

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

Is this a confidential response? (select as appropriate)

No

Video Game developers created sophisticated reporting routes for children and adults, allowing users to ban and report others on the sport. Additionally, companies also have proactive monitoring tools available that supervise game chats to look through keywords and phrases that might be offensive. Some companies also have a close relation with the police in how they escalate concerning content.

For example, a fundamental principle of Safety by Design is that any item or interaction generated by and shared to users of the service (aka User-generated content) can be flagged/reported intuitively and from the area of the user-interface where the viewing user was exposed to it. Reports or flags must then be sent to a human moderator to review the context and evidence in relation to how the content may be acceptable or not acceptable according to stated terms of service, and the community code of conduct contained therein. Companies also maintain that reporting mechanisms should also signpost alternate methods for users to resolve matters of undesirable online interactions or content, by presenting other tools such as blocking, muting, adjusting privacy settings etc. In order to gauge a user's understanding on how to use these functions, moderators track a 'validity' KPI which tracks the proportion of users that have used the tools for their intended purpose.

Another example of abuse reporting tools is a robust and formalised process for handling all reports, using a combination of ML/AI and human oversight. A human team manages

[6] https://www.askaboutgames.com/

[7] https://www.ipsos.com/en-uk/understanding-child-safety-and-video-gaming-gametrack

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

abuse reports, which is supported by Legal and Security teams. They work under a documented set of process and a disciplinary matrix, with an escalation process in place, including to report to law enforcement. These processes are designed by a combination of trust & safety specialists, Legal and Security with input from other internal and external stakeholders.

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Is this a confidential response? (select as appropriate)

No

The video games industry is actively working on maintaining a positive community in the game environment, for example by hiring community managers, whose role is to build self-sustaining, healthy, non-toxic communities that moderate themselves.

Often, they have specific Codes of Conduct or Terms of Use in place to fight against toxicity on their services, whereby mechanisms are implemented to detect and sanction toxic players (including permanent banning) or educational programs are set up in order to ensure a fair and friendly gaming environment for their players.

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Is this a confidential response? (select as appropriate)

No

As mentioned previously, sophisticated and robust parental control tools on a variety of devices and software applications allow parents to agree with their children, based on their age and maturity, what type of video game content can be accessed, whether in-game spending will be allowed or limited, or if any data may be shared with others online. Additionally, the parental controls and safety features allow users to restrict content, filter images and chat, restrict interaction etc according to any number of factors relevant to the individual.

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

To support the parent in the decision-making process of buying a game or adjusting the parental tools, the industry committed to adopt the PEGI system to protect minors and behave responsibly where children are concerned.

Each publisher that joins PEGI has to sign a Code of Conduct committing him to provide parents with objective, intelligible and reliable information regarding the suitability of a game's content. By signing the Code of Conduct, the publisher also undertakes to maintain a responsible advertising policy, provide opportunities for consumer redress, maintain community standards and adhere to stringent standards for a safe online gaming environment. These include the need to maintain an effective and coherent privacy policy which must encompass the responsible collection, distribution, correction, and security of the personal details of users who must be given the opportunity to comment on any perceived misuse of their personal details and therefore be fully advised as to ways, for example, of avoiding unsolicited or unwanted e-mail contact.

Additionally, in 2013, the industry established IARC, The International Age Rating Coalition, which comprises rating boards from Europe, North America, Brazil and Australia who have joined forces to provide a solution for the globalised market of apps collectively representing regions serving approximately 1.5 billion people. IARC has now been adopted by Google Play Store, Microsoft Windows Store, Nintendo® eShop and the Sony PlayStation® Store and informs the consumer about certain types of functionality in an app, such as in-app purchases, location data sharing, unrestricted internet access and the ability of users to interact.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

Is this a confidential response? (select as appropriate)

No

A video game company's priority is to build child and user protection into its systems by default and by design, varying from other online platforms which permit access to all content and then attempt to build functionalities onto their open-systems to try to protect users.

Because most potentially harmful content on the services is text based or communications related, they are best mitigated through a combination of AI + human oversight filtering and moderation plus abuse reporting. Our members believe that social features designed

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

to enhance the enjoyment of users' gaming experiences, also need to build in safety as part of their design. This includes requiring any social or user-generated content application or game to apply a number of integrated features such as user-reporting of any user-generated content, respecting a player's privacy settings, block lists and muting preferences, as well as (in the case of child accounts) whether the player's parent or guardian has set them to be able to communicate with other players. In some instances, companies build features that allow non-verbal communication, such as the Ping System for a popular multiplayer game. Features are also required to respect moderation decisions such as removal of content or restrictions placed on users' account access.

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

The designers of a video game constantly integrate new content detection and suppression technologies to text profanity and prohibited words, URLs and images. This reduces the risk of children interacting with content that could be deemed harmful to them.

Additionally, companies also provide information resources for particular issues to their users, including on bullying and abuse.

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?

Is this a confidential response? (select as appropriate)

No

NA

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Is this a confidential response? (select as appropriate)

No

We believe that we are doing everything possible to ensure an optimal balance between the safety of our community and the freedom of our users.

That said, the industry keeps investing in AI tools and human moderation to create a more sophisticated moderation regime that remains protective of the privacy and freedom of communication of our players.

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

See answer to Q17.

Question 22: How are human moderators used to identify and assess content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

Every game publisher or developer will have some level of moderation in place if their game is based on online play, often through human game moderators.

Game moderators are professional people hired to moderate games. They're responsible for maintaining online gaming platforms free from any inappropriate, illegal content. Moderators generally ensure that players follow the game's guidelines and rules, and they operate on a model of notice and take down.

Question 22: How are human moderators used to identify and assess content that is harmful to children?

Question 23: What training and support is or should be provided to moderators?

Is this a confidential response? (select as appropriate)

No

All moderators are trained in the requirements & guidelines they are expected to follow and practice certain situations on how they should respond. They are also trained in the moderation techniques and practices, as well as in the risks that can originate from a specific game/platform.

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?

Is this a confidential response? (select as appropriate)

No

Although AI moderation tools significantly reduce the need for manual moderation, these tools still need input from humans so they can constantly evolve while taking new words and language into account. Additionally, abuse from the use of sarcastic language will be difficult for AI to spot, and easy for a human moderator.

The most effective way to moderate gaming content generated in real-time is to combine human moderation and AI. The AI algorithm filters out content that meets specific criteria and passes on the content that requires human judgment to human moderators, reducing the workload for staff. This approach, which combines the strengths of humans and machines, is more productive, less biased, and cost-effective than relying solely on human moderators.

Question 25: In what instances is content that is harmful to children, that is in contravention of terms and conditions, removed from a service or the part of a service that children can access?

Is this a confidential response? (select as appropriate)

[Please select]

Members usually operate on a notice & take down, meaning if the user is reported by players, there is either automated temporary sanction; or a human review; which could lead to a short suspension of a chat feature, temporary ban, or definitive ban.

Additionally, the game chat is usually not permanent, so the content of the chat cannot be accessed later by the players (it might be stored in publisher systems for a certain amount of time).

Question 26: What other mitigations do services currently have to protect children from harmful content?

Is this a confidential response? (select as appropriate)

[Please select]

The information covered throughout this paper gives a comprehensive picture of the industry's approach. However, the industry is constantly working to develop and update its safety procedures, including partnering with other organisations and experts in this field.

Additionally, game developers also allow users to hide the real name of an account holder, showcasing only the username chosen by the individual. This is done to protect the identity of a user. The user has the ability to determine who is allowed to see their real name.

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

Is this a confidential response? (select as appropriate)

[Please select]

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

As previously mentioned, several platforms are testing various forms of age verification methods, allowing users to access innovative social capabilities and age-appropriate content while also ensuring the safety of their community. The platforms also have inbuilt tools to prevent children from changing parental controls. This is done via authentication methods, such as passcodes, requiring the primary account holder to approve requested changes.

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?

Is this a confidential response? (select as appropriate)

[Please select]

Overall, we believe to have demonstrated the extent to which the video game industry protects children in their online environments through their safety by design ideology. This protection commences at the design stage, when developers intentionally designs systems to provide a low-risk environment for all users. The measures extend to the parents or guardian, with the industry investing resources to develop tools and campaigns, including Ukie's Get Smart About PLAY, educating parents on how to best engage with parental tools which enables them to set the permissions that are appropriate for them or their children.

The parental tools are also supported through substantive device settings, which can only be changed by the primary account holder, thus making it difficult for children to amend any settings. In addition to the platform controls, video game publishers also include various measures into their game to prevent children from being exposed to harmful content, including the party and ping system, which provide the choice with whom to play, as well as how to interact with other players.

The designers of a video game also constantly integrate new content detection and suppression technologies to text profanity and prohibited words, URLs and images.

These measures are all supported through an advanced moderation system described in the answers above, which aids developers to sanction and ban players that promote harmful content.