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
The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR) and the Environmental Information Regulations 2004 (EIR). The ICO is independent from government and upholds information rights in the public interest, promoting transparency and openness and data privacy for individuals. In this response we refer to the ICO's Children's code (the Children's code or the code). The Children's code is a statutory code of practice published pursuant to s123 of the DPA18. The code applies to "Information Society Services likely to be accessed by children." It therefore applies to many apps, programs, search engines, websites, streaming services and online games, including services likely to be captured by the scope of the online safety regime. It sets out standards that services should conform to, to provide better privacy protections for children. If services do not conform to the code, they are likely to find it more difficult to demonstrate compliance with data protection law.

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
The Children's code requires Information Society Service Providers (ISS) to determine whether their service falls within scope of the Children's code. The code applies to ISS that are "likely to be accessed by children" in the UK. In September 2022, the ICO clarified that adult-only services are in scope of the Children's code if they are likely to be accessed by children. This means that the code applies: • to services that are intended for use by children; **and** • to services that are not specifically aimed or targeted at children, but are nonetheless likely to be used by under 18s.

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

Even if a service states in the terms of service that under 18s should not access the service, it may still fall within scope of the code if children access the site in practice.

The ICO is consulting on the following list of non-exhaustive factors that should be taken into account when carrying out an assessment of whether children are likely to access an ISS. This will be underpinned by guidance and case studies to support ISS to make this assessment.

Examples of factors to consider	**Notes and any limitations**
Actual evidence or information you have	
The number of child users of your service, and the proportion of total UK users or total UK children that this represents.	The number of UK child users may be considered significant in absolute terms or in relation to the proportion it represents of total UK users of the service or the number of children in the UK. Current UK population data should be used to assess the latter. Sources of evidence may include any age data you have available, such as data gathered from any age profiling tools you may be using.
Any research evidence available such as: - **Your own research about your users** - **Any existing evidence of user behaviour.**	Existing evidence of user behaviour may include internal analytics, business intelligence and market research, including data about a user or groups of users to estimate or infer the age, age range, or proxy thereof.
Information on advertising targeted at children.	This includes whether advertisements on your service, including third party advertisements, are directed at or are likely to appeal to children. You may have data, including data provided to or by advertisers, such as number of clicks on ads that show an interest in child-focused advertising.
Information on complaints received related to children	Information you receive regarding complaints from parents, children or third

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?	
accessing or using your service.	parties about the age of users accessing your service.
Other evidence to consider	
Consideration of the types of content, design features and activities children are interested in.	The subject matter or nature of the content on your service, including any data that estimates, identifies or classifies that the content is likely to be of interest to children. This includes if children are the intended, or likely part of the intended audience for the content. For example, cartoons, animation, music or audio content, incentives for children's participation, presence of children, influencers or celebrities popular with children.
Any other research evidence such as: - **Academic, independent and market research** - **Research relating to similar providers of ISS.**	This includes research you may have commissioned yourself, as well as publicly available research.
Consideration of whether children are known to like and access similar services.	Evidence of children accessing services with similar content.
Your operating/business model.	Information about your revenue streams and sources of turnover, as well as other information captured in management accounts or annual reports that suggests that children are an audience for your service, and that the service is likely used by a significant number of children.
How your service markets, describes and promotes itself.	For example, is any advertising targeted at children? Are there toys or other products associated with your services targeted at children?

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

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

Standard 3 of the Children's code says that organisations in scope should "take a risk-based approach to recognising the age of individual users" and "either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead." Services can also consider preventing access to children, where appropriate.

The Children's code is not prescriptive about how an organisation should establish the age of their users, but the method used to establish or verify age should be proportionate to the data processing risks that may arise from the processing of children's personal data. Age assurance measures that can be considered by organisations may include:

- Self-declaration
- Artificial intelligence
- Third party age verification services
- Account holder confirmation
- Technical measures
- Hard identifiers

The above examples are described in further detail in the Children's code itself.

The ICO has published a Commissioner's Opinion on age assurance for the Children's code (the Commissioner's Opinion). This opinion sets out how organisations should approach age assurance to conform to the Children's code and comply with data protection law.

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

Age assurance measures are rapidly developing and can vary in the volume of personal data required to operate them effectively, as well as in their accuracy and cost. There are a range of age assurance tools available to platforms, including age estimation techniques that use biometric facial scans, iris scans, or voice scans. Age verification techniques can include the use of hard identifiers such as passports, driving licences or, another verifiable record of age. Other techniques include the use of self-declaration of age.

Annex 2 of the Commissioner's Opinion provides a summary of the ICO's assessment of uses of age assurance (as at the date of publication of the Opinion in October 2021).

Annex 3 of the Commissioner's Opinion contains an economic analysis of the impact of age assurance at the date of its publication (October 2021).

The ICO's response to its call for evidence on age assurance provides a summary of the views of stakeholders we engaged with in late 2021 and early 2022, and the concerns raised about age assurance measures which were available at that point.

The ICO continues to develop its position on age assurance and has undertaken research, including in tandem with Ofcom, to explore how efficacy of age assurance measures can be determined, and families' attitudes to age assurance more broadly. These research pieces will inform further work in this area.

Data Protection Impact

The Children's code requires organisations in scope to take a risk-based approach to using age assurance techniques to ensure the technique deployed is proportionate to the risks arising from their use of children's data.

Under standard 2 of the code, Data Protection Impact Assessments (DPIAs) should be undertaken to assist organisations in identifying data protection risks to users, the harms this can lead to, and to implement appropriate mitigating measures, including age assurance measures. We set out more details in our response to question 8 below. The Commissioner's Opinion states that to meet the necessity threshold in data protection law, organisations have to demonstrate that the age assurance measures deployed are effective in achieving their purposes.

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?

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)

[Please select]

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)

[Please select]

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

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

In order to conform to the Children's code, organisations in scope should ensure the primary focus is on the best interests of the child when designing and developing online services children are likely to access. To do this, an organisation needs to carry out a DPIA and a 'best interests of the child assessment' should be carried out as part of this exercise.

DPIA

To conform to Standard 2 of the Children's code, a DPIA should be undertaken in order to identify, and take appropriate steps to, mitigate the risks to the rights and freedoms of children and this should consider the differences between children of different ages, their levels of understanding and their development needs so that measures can be implemented to ensure conformance with the rest of the Children's code. As part of this assessment, an organisation should consider the potential impact on children and any harm that may be caused by the data processing activity. The likelihood and severity of this impact needs to be considered in order to assess the level of risk and mitigate the risk. This mirrors the approach outlined within the ICO's Harms Taxonomy.

Best interests of the child assessment

Standard 1 of the Children's code requires organisations in scope to ensure the best interests of children is the primary consideration when designing and developing online services that children are likely to access. This is derived from Article 3 of the United Nations Convention on the Rights of the Child (UNCRC).

There is a four-step process to the best interests of the child assessment:

1. **Understand the rights children hold under the UNCRC**
   E.g. children's right of access to leisure, play and culture, and children's right to privacy.

2. **Identify the impact of processing on children's rights**

   E.g. age assurance can impact a child's right to privacy if data gathered for age assurance is used for a different purpose

3. **Assess the impact that processing will have on children's rights**

   This should be evidence based, and services are encouraged to use the ICO self-assessment risk tool to assess the level of risk the processing activity poses

4. **Prioritise how to reduce the risks identified in step 3**

   E.g. actions ISS can take may include ensuring only the minimum amount of data is collected for age assurance, and ensuring this data

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?
isn't used for any other purpose. The best interests of the child assessment requires an organisation to identify and assess the impact of data processing activities on children's rights. This assessment, carried out as part of their DPIA, therefore requires them to consider the harms that may arise from these processing activities, such as online grooming, excessive screen time, and social anxiety. The ICO's Harms Taxonomy provides ISS with a broad framework they can refer to in order to identify such harms.

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
Under data protection law when considering the risks to children using online services, organisations should consider the data protection risks that may arise due to the specific data processing activity being carried out, alongside the impact and/or harms that may be caused to children as a result. Risk factors that may result in a risk to children may include data processing activities where they are not carried out in the best interests of the child, such as: - Online tracking - Profiling - Data sharing Conformance to the 15 standards in the Children's code should largely mitigate such data processing risks as it centres on the use of high privacy by default settings for users under the age of 18 and requires organisations to carry out a DPIA to identify and mitigate these risks. The code also requires organisations to consider the best interests of children when designing and developing their services (see response to question 8). The Children's code Self-Assessment Risk Tool and the Best Interest of the Child Self-Assessment Tool are additional resources that can also be used by organisations to conduct their own risk assessment on their own platform and/or service. These resource also provides examples of the practical steps that can be taken by organisations to ensure a risk-based approach is adopted to support children's privacy.

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

Data protection law contains accountability requirements. Further information about data protection governance requirements is available here: [Governance and accountability | ICO,]()

Under the Children's code organisations in scope should have relevant systems in place to support and demonstrate compliance with data protection legislation and conformance to the code.

The Children's code states that organisations should undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access the service. More information is set out in our response to question 8.

Organisations should be prepared to demonstrate compliance with data protection law, including conformance with the code, to the ICO if necessary. Examples of how this can be demonstrated are DPIAs, relevant policies, training records, and records of processing activities.

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

Drafting Effective Privacy Information Under the UK GDPR,

Under data protection law services are required to provide individuals with privacy information about their personal data processing in a way that is easily accessible and easy to understand, using clear and plain language. The ICO's Guide to Data Protection provides practical guidance about how privacy information should be drafted. Among other measures, it recommends that user testing is carried out on privacy information to get feedback on how easy it is to access and understand. It also recommends that, when drafting privacy information, organisations should put themselves in the position of the user that they are collecting information about. The Guide to Data Protection also refers to techniques that can be used to provide clear and accessible privacy information. These include using:

- A layered approach - short notices containing key privacy. information that have additional layers of more detailed information

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)?

- Dashboards - preference management tools that inform people how organisations use their data and allow them to manage what happens with it.
- Just-in-time notices - relevant and focused privacy information delivered at the time organisations collect individual pieces of information about people.
- Icons - small, meaningful symbols that indicate the existence of a particular type of personal data processing.
- Mobile and smart device functionalities - including pop-ups, voice alerts and mobile device gestures.

The ICO's Accountability Framework is an additional resource setting out how services can meet the ICO's expectations for transparency and clarity.

The Children's Code

Standard 4 of the Children's Code requires that the privacy information (and other published terms, policies and community standards) that services provide to child users must be concise, prominent, and in clear 3 language suited to the age of the child. Services should provide additional specific 'bite-sized' explanations about how they use personal data at the point that use is activated. Information should be tailored to the age of the child/user. The code provides some detail, including:

- Services should present all this information in a way that is likely to appeal to the age of the child who is accessing their online service. This may include using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest children, rather than relying solely on written communications.
- Services may use tools such as privacy dashboards, layered information, icons and symbols to aid children's understanding and to present the information in a child-friendly way.
- Services should take an evidence-based approach to what methods of presentation are most appropriate for their service. This could include consulting with children and parents, referring to best practice design methods or academic research, analysing user redress and feedback data, engaging with children's development and rights specialists or using external audits.

Best Practice in Service Design

The ICO has published recommendations for designing data transparency for children. This report celebrates current good practice and showcases the 'art of the possible' when it comes to creating data transparency for children. The ICO's award winning Children's Code design guidance shows how to apply the Children's Code in practice and includes tools that organisations can use to create an open, transparent and safe place for children online.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[1]
Is this a confidential response? (select as appropriate) *[Please select]*

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

Standard 15 of the Children's code requires organisations in scope to provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

Online tools are mechanisms to help children exercise their rights simply and easily when they are online.

In order to comply services in scope of the Children's code need to find ways to make sure that children know about their data protection rights and are able to easily exercise them. They have an obligation not just to allow children to exercise their rights but to help them to do so. The code sets out the following requirements:

Make tools prominent.

The tools that are provided to help children exercise their rights and report concerns must be easy for the child to find. Services should highlight the reporting tool in their set up process and provide a clear and easily identifiable icon or other access mechanism in a prominent place on the screen display.

Make them age appropriate and easy to use.

Tools should be age appropriate and easy to use. Services should therefore tailor them to the age of the child in question. The Children's code includes some guidelines. However, these are only a starting point and services are free to develop their own, service specific, user journeys that follow the headline standard.

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

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

Age range	Recommendations
0-5 Pre-literate & early literacy	Provide icon(s), audio prompts or similar that even the youngest of children will recognise as meaning 'I'm not happy' or 'I need help'. If these buttons are pressed, or other prompts responded to, provide video or audio material prompting the child to get help from a parent or trusted adult. Provide online tools suitable for use by parents.
6-9 Core primary school years	Provide icon(s), audio prompts or similar that children will recognise as meaning 'I'm not happy' or 'I need help'. If these buttons are pressed, or other prompts responded to, provide video or audio material prompting the child to get help from a parent or trusted adult, then direct the child to your online tool. Provide online tools that children could use either by themselves or with the help of an adult.
10-12 Transition years	Provide icon(s), audio prompts or similar that children will recognise as meaning 'I'm not happy' or 'I need help'. If these buttons are pressed, or other prompts responded to, direct the child to your online tool and prompt them to get help from a parent or trusted adult if they need it. Provide online tools that children could use either by themselves or with the help of an adult.
13 -15 Early teens	Provide icon(s), audio prompts or similar that children will recognise as meaning 'I want to

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

	raise a concern’ ‘I want to access my information’ or ‘I need help’. If these buttons are pressed, or other prompts responded to, direct the child to your online tools and prompt them to get help from a parent or other trusted resource if they need it. Provide online tools suitable for use by the child without the help of an adult.
16-17 Approaching adulthood	Provide icon(s), audio prompts or similar that children will recognise as ‘I want to raise a concern’ ‘I want to access my information’ or ‘I need help’. If these buttons are pressed, or other prompts responded to, direct the child to your online tools and prompt them to get help from a parent or other trusted resource if they need it. Provide online tools suitable for use by the child without the help of an adult.

Make your tools specific to the rights or facility they support.

Include mechanisms for tracking progress and communicating with the service.

Online tools can include ways for the child or their parent to track the progress of their complaint or request and communicate with the service about what is happening.

Services should provide information about their timescales for responding to requests from children to exercise their rights and should deal with all requests within the timescales set out at Article 12(3) of the UK GDPR.

Services should have mechanisms for children to indicate that they think their complaint or request is urgent and why and should actively consider any information children provide in this respect and prioritise accordingly. Services should have procedures in place to take swift action where information is provided indicating there is an ongoing safeguarding issue.

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)

[Please select]

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)

[Please select]

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

Please see our response to Q17 for more information on some of the features/ functionalities services should consider. The Commissioner's Opinion highlights some existing measures which may be deployed to ensure that children's personal data is provided added protection and they have appropriate experiences online.

Alternatively, the Children's code is clear that organisations can choose to apply all 15 standards of the code to all users, regardless of their age.

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

The ICO's Guide to Data Protection recommends that organisations offer strong privacy defaults for all users as part of a data protection by design and default approach.

The Children's code places an emphasis on the use of high privacy by default settings for under 18's. These can contribute to child safety online in a broad sense. For example:

Standard 7 of the code requires services to set privacy settings to high privacy by default unless they can demonstrate a compelling reason for a different default setting taking into account the best interests of the child. High privacy by default settings can mean that children's personal data is only visible or accessible to other users of the service if the child (or a parent or guardian) actively amends their settings -this may help to reduce unwanted communications with people that children do not already know.

High privacy by default settings may also mean that, unless a setting is changed, a service's own use of the children's personal data is limited to that which is essential to the core provision of the service. Any optional or supplementary uses of personal data, potentially including any processing to personalise the service, have to be individually selected and activated by the child.

Standard 11 covers parental controls which can be put in place for parents to place limits on a child's online activity and mitigate the risks that the child might be exposed to. It recognises this has privacy implications for children and cautions that where parental monitoring is happening, this should be made clear to children through age-appropriate information.

Standard 12 requires services to turn off profiling by default unless services can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child. The code notes that some profiling may be relatively benign but other profiling, such as personalised content feeds that gradually take a child away from their original area of interest into other less suitable content, raise more significant concerns.

Standard 13 of the Children's code refers to nudge techniques. These are defined as design features which lead or encourage users to follow the designer's preferred paths in the user's decision making.
The Children's code envisages that nudge techniques can be used for pro-privacy reasons, for example nudging towards high privacy options where this

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 appropriate, taking into account the best interests of the child. The code also suggests that services should consider nudging to promote the health and wellbeing of child users. For example, nudging children towards supportive resources where necessary. The code sets out recommendations about how such tools might be tailored to the age range of different child users.

The use of nudge techniques in the design of online services can also have negative effects on privacy where they encourage users to provide more personal data than they would otherwise volunteer. Standard 13 requires that services should not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections. This requirement reflects data protection law generally as it applies to all users, including adults.

Best Practice in Service Design

The ICO's Children's code design guidance contains design guidelines for protecting children's privacy by default and also references "things to avoid," such as nudge techniques that influence children towards sharing their personal data. One of the tools in the design guidance helps organisations identify the 'risky moments' in their service where supportive design features can help minimise the risk posed to children.

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)

[Please select]

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

The ICO has recently refreshed its [Guidance on AI and Data Protection]() (refreshed on 15 March 2023) which sets out what the ICO thinks is best practice for data protection-compliant AI, and how we interpret data protection law as it applies to AI systems that process personal data.

The guidance is of broader scope than the specific issues raised by the question but may provide a useful reference point for Ofcom to consider. Among other matters it covers issues such as fairness and transparency as they apply under data protection law.

Standard 12 of the code requires that profiling should be off by default unless it is in the best interests of a child.

It is important to acknowledge that the deployment of algorithms may not always be detrimental to children and could be in the best interests of children if the intention is for safeguarding and to suggest and recommend content that is appropriate to them, including any support services which may be required. It could also be used for age assurance.

As the use of algorithms for behavioural profiling to estimate an individual's age may increase, there is also a question of whether platforms will be able to ensure there is a clear demarcation in their use of data for different purposes, so there is no repurposing of data or function creep.

The use of algorithms should be accompanied with adequate transparency, so individuals are aware of how their data may be processed. However, when they are used for age assurance, it could be argued that transparency may assist individuals in circumventing and 'gaming' the system. A balance needs to be struck between transparency requirements and ensuring that an age assurance measure remains effective.

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)

[Please select]

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

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)

[Please select]

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)

[Please select]

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

Is this a confidential response? (select as appropriate)

[Please select]

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

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)

[Please select]

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]

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]

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

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)

No

The ICO is aware, from research commissioned jointly with Ofcom via the DRCF, and other sources, that children routinely circumvent self-declaration age requirements that are used widely on online services. The research also showed that parents will often assist children to circumvent these measures.

As it can be easily circumvented, self-declaration does not significantly mitigate risks to children, as explained in the Commissioner’s Opinion. The following mitigations can strengthen self-declaration:

- preventing the user from immediately attempting to re-register if they are denied access on first declaration; or
- closing the accounts of users discovered to be underage.

Standard 3 of Children’s code notes that internet services should ‘establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing or apply the standards in this code to all your users instead’. Another means of protecting children who may attempt to circumvent mitigations in place on a service would be to apply all the standards of the Children’s code to all users. Alternatively, services could create what Epic Games refers to as Cabined Accounts, which allow children to use a service without access to higher risk elements of the service that are enabled only after verifiable parental consent or the user passing through a more accurate age assurance system.

Services could also look to utilise different forms of age assurance, such as biometric age estimation, to reduce reliance on less accurate and effective systems such as self-declaration.

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]