Call for evidence response form

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
BSI is the UK's National Standards Body, incorporated by Royal Charter and responsible independently for preparing British Standards and related publications and for coordinating the input of UK experts to European and international standards committees. BSI has over 115 years of experience in serving the interest of a wide range of stakeholders including government, business and society. BSI represents the UK view on standards in Europe (via the European Standards Organizations CEN and CENELEC) and internationally (via ISO and IEC). BSI has a globally recognised reputation for independence, integrity and innovation ensuring standards are useful, relevant and authoritative. BSI is appointed by government and responsible independently for maintaining the integrity of the national standards-making system not only for the benefit of UK industry and society but also to ensure that standards developed by UK experts meet international expectations of open consultation, stakeholder involvement and market relevance. British Standards and UK implementations of CEN/CENELEC or ISO/IEC standards are all documents defining best practice, established by consensus. Each standard is kept current through a process of maintenance and review whereby it is updated, revised or withdrawn as necessary. Standards are designed to set out clear and unambiguous provisions and objectives. Although standards are voluntary and separate from legal and regulatory systems, they can be used to support or complement legislation.

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) *[Please select]*

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?
No comment.

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) *[Please select]*
No comment.

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) *[Please select]*
No comment.

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

There is value in creating codes of practice and standards that are technology agnostic to help platforms understand how they can mitigate risk. See question 18 response on details of work currently in development by BSI on age assurance.

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]

No comment.

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]

No comment

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)

[Please select]

No comment.

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)

[Please select]

No comment

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

Standards are a valuable tool for governance of emerging technology. Regulation may be an appropriate solution when bringing about change; however, in certain circumstances, regulation can be expensive to meet and to enforce, and it can also struggle to keep pace with innovation in an emerging field.

The use of standards as the basis of industry self-regulation, which can be combined with accredited conformity assessment where needed, gives confidence that certain behaviours are being followed.

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

Standards can be used to support government policy in a number of ways, including self-regulation, earned recognition and co-regulation

BSI has been engaging with the ICO on their Age Appropriate Design code. The Children's code (or the Age appropriate design code) contains 15 principles that online services need to follow. This ensures they are complying with their obligations under data protection law to protect children's data online.

In addition, we have been supporting the work of Baroness Beeban Kidron OBE, and 5Rights. The 5Rights framework was written to offer a single, principled approach that could be used to set a standard by which young people are treated in the digital world. Through this work there is an approach to reduce harm to children, while maintaining their rights and their online experiences.

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

- Age restrictions, minimum age limits (depending on the type of services, for e.g. purchasing items)
- Ease of reporting data breaches.
- Create a triage system to handle content reports.
- Setting default controls for age groups, e.g. primary schoolers, teenagers etc.

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]

[1] 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?[1]

No comment

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

- Educate children on the types of reporting services.
- Add an easy and accessible function onto websites and services to report children abuse content or any illegal content.
- Provide a list of the relevant public authorities.

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

There are a number of international examples that can be built on. For example, Australia’s Online Safety Act 2021; Online service providers are required to report on how they are implementing the Basic Online Safety Expectations (BOSE) as and when these reports are requested by the eSafety Commissioner. Based on the first set of responses from industry, published by eSafety in December 2022, we now have better knowledge of what steps platforms are taking to protect children from abuse and exploitation on the internet.

Singapore has long implemented a single Login for all citizens called Singpass termed the National Digital Initiative to facilitate transactions online with the public and private sector. They have a national certification authority which issues signing certificates and

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?

authentication certificates. It is worth evaluating whether the UK needs to adopt a similar approach.

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

There may be an opportunity to establish a governance structure or framework that manages errant companies or service providers. For example:
Stage 1: Issue warnings
Stage 2: Authority on child online safety should follow up on the corrective actions taken to address the issue
Stage 3: Suspend service providers' licence the offence is repeated.

BSI would welcome the opportunity to bring together stakeholders that can explore how a new framework for reporting can be developed that defines "good practice" for industry users to adopt.

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)

[Please select]

No comment

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)

[Please select]

No comment

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

There are a number of standards that service providers can use to help reduce risk of harm. The UK is leading the standards development work programme of two international Age Assurance Standards that provide guidance for platforms.

- ISO/IEC NWI 27566 "Information security, cybersecurity and privacy protection — Age assurance systems — Framework"

This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about age or an age range of a natural person.

- ISO/IEC PWI 7732, "Information security, cybersecurity and privacy protection — Age assurance systems — measurement and Testing"

The Department for Science Innovation and Technology (DSIT), The Information Commissioner's Office (ICO) and Ofcom are actively engaged panel members and are contributing to this standard to help shape its use in support of upcoming legislation.

The standard will help platforms;

- define the key terms, definitions and abbreviations applicable to the age assurance process
- identify indicators of confidence associated with age assurance systems

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

- specify the roles, responsibilities and procedures of key actors in the age assurance process, including the requirement to establish age assurance policies
- consider attack vectors and countermeasures (i.e. anti-spoofing techniques), presentation attack detection, algorithms, or sensors;
- define a common specification for how source(s), output(s), indicators(s) of confidence and a basis for a trust framework are established and communicated to other actors in the age assurance process, sharing, swapping or communicating the verified attributes/credentials
- identify the data protection, privacy and security objectives specific to the age assurance process

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)

[Please select]

No comment

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]

No comment

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]*
No comment

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]*
No comment

Question 23: What training and support is or should be provided to moderators?
Is this a confidential response? (select as appropriate) *[Please select]*
No comment

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]

No comment

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]

No comment

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]

No comment

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]

No comment

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)

No

In addition, to the standards noted above. There are standards that look to embed security into the system.

ISO 31700-1:2023 Consumer protection — Privacy by design for consumer goods and services is a new consumer led international standard that establishes high-level requirements for privacy by design to protect privacy throughout the lifecycle of a consumer product, including data processed by the consumer.

Consumers are a key stakeholder in the development of standards. BSI's open, consensus-based standards process ensures that their views are taken into account alongside those of industry and other stakeholders.

BSI's Consumer & Public Interest Network (CPIN) represents the views of UK consumers. It provides an independent consumer voice in the development of standards. CPIN members are volunteers, trained in consumer issues, who represent UK consumers in standards developing committees.

Digital is one of CPIN's priority areas. The balance between the benefits and potential harm of a rapidly expanding digital world can easily tip the wrong way; international solutions need to be delivered. CPIN have identified 4 main types of risks of consumer harm in a digital world;
o Physical harm; this may be through direct use, such as health problems caused by spending too much time at a computer, or indirect risks as the result of critical digital

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?

systems failing or being hacked, such as health services that rely on a digital harm, or autonomous vehicles.

o Emotional harm; failure to adequately police what is published online can result in cyber-bullying, online child abuse and the spread of terrorist or racist content. Emotionally damaging content can in turn cause physical harm to vulnerable consumers.

o Financial harm; the ability to make easy and seamless digital purchases, unhindered by physical interventions run the risk of a consumer running up debt - for example in online gambling. In addition to this, cybercrime and hacked data can be used by criminals to commit ID theft, while fraudsters care increasingly targeting victims through email, SMS and social media.

o Risks to the privacy of personal data; consumers must frequently provide significant personal details for products and services to work, yet few consumers fully understand how their information may be used by organisations that gather it. This risks their data being used in ways they wouldn't expect or want – for example being targeted by marketing based on profiling.