Information Commissioner's Office

Consultation:

Age Appropriate Design code

Start date: 15 April 2019

End date: 31 May 2019

ico.
Information Commissioner's Office

Introduction

The Information Commissioner is seeking feedback on her draft code of practice Age appropriate design - a code of practice for online services likely to be accessed by children (the code).

The code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet.

The code is now out for public consultation and will remain open until 31 May 2019. The Information Commissioner welcomes feedback on the specific questions set out below.

Please send us your comments by 31 May 2019.

Download this document and email to:
ageappropriatedesign@ico.org.uk

Print off this document and post to:
Age Appropriate Design code consultation
Policy Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation please telephone 0303 123 1113 and ask to speak to the Policy Engagement Department about the Age Appropriate Design code or email ageappropriatedesign@ico.org.uk

Privacy statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public or a parent). All responses from organisations and individuals responding in a professional capacity (e.g. academics, child development experts, sole traders, child minders, education professionals) will be published. We will remove email addresses and telephone numbers from these responses but apart from this, we will publish them in full.

For more information about what we do with personal data, please see our [privacy notice](#).

Section 1: Your views

Q1. Is the '**About this code**' section of the code clearly communicated?

Yes
We commend and affirm this proposed code of practice for Information Society Service providers. Only a comprehensive adoption of these proposed guidelines will achieve the Government's stated ambition for the United Kingdom (UK) to become the safest place in the world to go online and the best place in the world to grow a digital business. Protecting children from harm is a principle of duty-of-care that must guide, rather than be controlled by, current or emerging technological challenges. Children cannot protect themselves and because self-regulation has clearly failed to provide adequate protection on their behalf, we recommend these draft guidelines as appropriate and proportional.
        as the Bishop of Chelmsford notes:

"The digital age can be an age of cultural, intellectual and even moral prosperity, but enlightened legislation based on sound and child-centred research is needed to lift it from the mire and misery it is also creating. This will require great determination from the Government, but perhaps the first step is to acknowledge that self-regulation does not work. Commercial interest always outflanks care of the child. This must change, and the Government must take a lead. It is often said of government that its first responsibility is to protect citizens. We should now ask our Government to protect our children."

The Lord Bishop of Chelmsford, HL Deb November 7, 2019, vol 785 c1747.

Q2. Is the '**Services covered by this code'** section of the code clearly communicated?

No
 Although the reference to services "likely to be affected" is good, there is too much ambiguity in the term "likely to be accessed by children". We agree that children must have their settings moved to 'high privacy' by default and we therefore require improved clarity over the use of the word 'likely' and the inclusion of example services. For instance, it is not clear what 'documented evidence' will satisfy the proposed test for exclusion. The draft guidelines would also benefit from clarifying their scope since both gambling and streaming services, even where their terms of service specifically exclude under-18 years olds can, in practice, be expected to be 'likely to be accessed' by under-18 year olds unless robust exclusion and age-verification procedures are put in place.

Standards of age-appropriate design

Please provide your views on the sections of the code covering each of the 16 draft standards

1. Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

2. Age-appropriate application: Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

3. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

4. Detrimental use of data: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

5. Policies and community standards: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

6. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

7. Data minimisation: Collect and retain only the minimum amount of personal data necessary to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

8. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

9. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

10. Parental controls: If you provide parental controls give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

11. Profiling: Switch options based on profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

12. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off privacy protections, or extend use.

13. Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable compliance with this code

14. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

15. Data protection impact assessments: Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

16. Governance and accountability: Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code

Q3. Have we communicated our expectations for this standard clearly?

1. **Best interests of the child**
Yes
This is a principle we strongly affirm. There is recent evidence that young people are devaluing their own privacy and safety because of their low expectations over treatment by social media platforms.

BCS, The Chartered Institute for IT, Survey: Children's Views on Internet Safety, 2018, p. 3, accessed May 16, 2019. https://www.bcs.org/upload/pdf/internet-safety-results.pdf.

2. Age-appropriate application

Yes

 This too is an important principle. Limiting content in an age-appropriate way depends upon robust mechanisms for verifying the user's age. Clearly, current solutions are not working and undermine trust in the tech sector. The case for this draft Code's proportionate and risk-based approach to age-verification is overwhelming. Dilution of that principle would risk two consequences. First it would increase the difficulty of identifying the 'best interests' of individuals under 18 years of age accessing digital services. Secondly, dilution would diminish the commercial opportunities this provision invites for technological innovation in the digital world. Without a robust and rigorous age-verification mechanism, the duty of care principle that underpins these guidelines cannot be implemented.

the Lord Bishop of Chelmsford has noted that:
"An unregulated digital environment is causing moral decay. There is no time to reiterate the various harms that are being caused, but they are deep-seated, corrosive and pervasive. Just last week I was at a school in Essex talking to seven to eleven year-olds about their use of a game called TikTok. All of them were using it. The lower age limit for using it is 13. […] the digital world assumes that all users are equal, and all users are adults, whereas in fact one-third of users worldwide are children. Therefore, their health, well-being and development require us to ensure that the internet, and the many ways that children access it, are as safe as they can be. This has usually meant creating special safe places for children or safety options that can be activated."

The Lord Bishop of Chelmsford, HL Deb January 17, 2019, vol 795 c408.

3. Transparency

Yes

4. Detrimental use of data

Yes

5. Policies and community standards

Yes

Under-18s comprise at least 20 per cent of UK internet users. The Church's own safeguarding policies affirm the belief that all human beings are created in God's image and that children fully deserve to be treated with dignity, care and compassion. These draft proposals are commendable for recognising the distinctive vulnerabilities and special needs of children. However,

The best interests of the child are only one aspect of a greater "common good"; 'The principle of the common good, to which every aspect of social life must be related if it is to attain its fullest meaning, stems from the dignity, unity and equality of all people. […] The common good does not consist in the simple sum of the particular goods of each subject of a social entity. Belonging to everyone and to each person, it is and remains "common", because it is indivisible and because only together is it possible to attain it, increase it and safeguard its effectiveness, with regard also to the future.'

(Compendium of the Social Doctrine of the Church, (164)).

6. Default settings

Yes

75 per cent of young people also think social media companies should automatically block offensive and abusive messages. 'Children, and younger children particularly, are in favour of social media platforms removing offensive or abusive content or direct messages automatically, without the need for a user complaint to be made first, and for this to be a default setting. As might be expected, the older the children become, the less sure they are that they want to be shielded from offensive or abusive content.'
BCS, survey: Young People and Bullying on Social Media Social Survey, 2018, accessed May 22, 2019, https://www.bcs.org/upload/pdf/internet-safety-results.pdf.

7. Data minimisation

Yes

8. Data sharing

Yes

9. Geolocation

Yes

10. Parental controls

Yes

11. Profiling
Yes

12. Nudge techniques
No   While the draft code's DPIA template includes the question, "Does your service use any nudge techniques?" the draft is, again, short on both detail and examples. Dark nudges and 'sludge' (the practice of making commercially unwelcome features onerous to utilise) are already having tangible effects on the well-being of children. See The 5Rights Foundation report, Disrupted Childhood, 2018, accessed May 21, 2019, https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf.

13. Connected toys and devices
Yes

14. Online tools
Yes

15. Data protection impact assessments
Yes

16. Governance and accountability
Yes

Q4. Do you have any examples that you think could be used to illustrate the approach we are advocating for this standard?

1. **Best interests of the child**
Yes

The Church of England's own safeguarding policies affirm the belief that all human beings are created in God's image and that children fully deserve to be treated with dignity, care and compassion.

Church of England Report, All God's Children, 2010, SS 1.6ff, accessed May 16, 2019, https://www.churchofengland.org/sites/default/files/2017-11/protectingallgodschildren.pdf.

 This conception of proportional responsibility for the common good is deeply embedded in the Christian tradition through its emphasis on practical love for neighbour and theological understanding of every person is an interconnected member of an overarching 'body.'

2. Age-appropriate application

Yes

 This is needed because "An unregulated digital environment is causing moral decay. There is no time to reiterate the various harms that are being caused, but they are deep-seated, corrosive and pervasive. Just last week I was at a school in Essex talking to seven to eleven year-olds about their use of a game called TikTok. All of them were using it. The lower age limit for using it is 13. […] the digital world assumes that all users are equal, and all users are adults, whereas in fact one-third of users worldwide are children. Therefore, their health, well-being and development require us to ensure that the internet, and the many ways that children access it, are as safe as they can be. This has usually meant creating special safe places for children or safety options that can be activated."

The Lord Bishop of Chelmsford, HL Deb January 17, 2019, vol 795 c408.

There is recent evidence that young people are devaluing their own privacy and safety because of their low expectations over treatment by social media platforms.

BCS, The Chartered Institute for IT, Survey: Children's Views on Internet Safety, 2018, p. 3, accessed May 16, 2019.
https://www.bcs.org/upload/pdf/internet-safety-results.pdf.

3. Transparency

No

4. Detrimental use of data

Yes

Rather than considering the 'best interests of the child' as these proposed guidelines correctly propose, protecting children has been made harder by the tech industry's adoption of psychological tools to design compulsive and potentially addictive services. The Chief Medical Officer has evaluated screen-based activities, finding excess exposure detrimental to children's sleep, concentration, and mood.

United Kingdom Chief Medical Officers' commentary on 'Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews', February 2019, accessed May 17, 2019, https://www.gov.uk/government/publications/uk-cmo-commentary-on-screen-time-and-social-media-map-of-reviews.

"It has been encouraging that the Gambling Commission has taken a stronger line on an industry that in the past performed abysmally in its duty of care to its customers. If companies such as Facebook, Snapchat or YouTube are to behave, the regulators will need to have significant powers and there will need to be real independence. […] some cynics have been arguing that some of these companies simply budget in the fines as part of their ongoing business so that they can keep going as they have in the past. […] Therefore, there is a question about not only how we regulate them but how we get them to engage with the wider debate about the sort of world we want to create."

The Lord Bishop of St. Albans, HL Deb April 30, 2019, vol 797 c908-9.

5. Policies and community standards

Yes

The tech industry appeals to 'exceptionalism' in order to separate its own behaviour from that permitted in the offline world while conventional economic models explain how the profit motive incentivises a race to the bottom where 'dark nudges' exploit vulnerability that harms individual users and imposes economic costs on society.

Philip W. S. Newall, 'Dark Nudges in Gambling', Addiction Theory and Research, Vol. 27, Issue 2, (2018), 65-67, accessed May 16, 2019, https://doi.org/10.1080/16066359.2018.1474206.

The Lord Bishop of Gloucester has highlighted the damaging consequences of digital platforms absolving themselves of responsibility for access to content:
"The content we consume shapes how we see ourselves, other people and the world. It is no longer sufficient for social media and online platforms to cling to a simple dichotomy of platform versus publisher in

order to escape responsibility for the content they promote and share. While previous generations' engagement with media might have been limited to print media and television broadcasts regulated by formal standards and watersheds, modern consumers, including children, are exposed to huge swathes of unregulated content. Research conducted by the UK Safer Internet Centre in 2016 found that more than 80 per cent of the teenagers surveyed had seen or heard online hate about a specific group."

The Lord Bishop of Gloucester, HL Deb January 11, 2019, vol 788 c376.

6. Default settings:

Yes

  Primary care givers provide protection to children, but few can keep up with the demands of technological developments, least of all carers who may, themselves, be vulnerable adults. Parents repeatedly call for better protection by the tech sector itself.

Ofcom, report: Children and Parents Media use and Attitudes 2018, January 2019, accessed May 23, 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf.

But 75 per cent of young people also think social media companies should automatically block offensive and abusive messages.
Children, and younger children particularly, are in favour of social media platforms removing offensive or abusive content or direct messages automatically, without the need for a user complaint to be made first, and for this to be a default setting.

BCS, survey: Young People and Bullying on Social Media Social Survey, 2018, accessed May 22, 2019, https://www.bcs.org/upload/pdf/internet-safety-results.pdf.

As might be expected, the older the children become, the less sure they are that they want to be shielded from offensive or abusive content.

Ibid. p.4.

7. Data minimisation

Yes

  Age-verification must also respect the child's privacy, affording them space to develop their own sense of personhood and identity. As the Lord Bishop of Gloucester has said:
"I have had the privilege of meeting young people in primary and secondary schools in Gloucestershire, and much of what I have heard from them resonates with the recommendations of this report. As the

report highlights, children live in a world where being online is interwoven with every aspect of their everyday lives, and young people do not want discussion about the internet always to begin from an angle of prohibition. It is undoubtedly good that there is a clear commitment to keep children and young people safe online. We need child-centred design, a code of practice and adequate procedures, but all that must sit within a wider context of human flourishing and human relationship."

The Lord Bishop of Gloucester, HL Deb November 7, 2017, vol 785 c1756

To that end we also strongly affirm the Code's principles concerning data minimisation and data sharing.

8. Data sharing
No   If YES, then please provide details.
9. Geolocation
No   If YES, then please provide details.
10. Parental controls
Yes   Primary care givers provide protection to children, but few can keep up with the demands of technological developments, least of all carers who may, themselves, be vulnerable adults. Parents repeatedly call for better protection by the tech sector itself. Ofcom, report: Children and Parents Media use and Attitudes 2018, January 2019, accessed May 23, 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf.
11. Profiling
No   If YES, then please provide details.
12. Nudge techniques
Yes   While the draft code's DPIA template includes the question, "Does your service use any nudge techniques?" the draft is, again, short on both detail and examples. Dark nudges and 'sludge' (the practice of making commercially unwelcome features onerous to utilise) are already having tangible effects on the well-being of children.   The 5Rights Foundation report, Disrupted Childhood, 2018, accessed May 21, 2019, https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf.

The tech industry appeals to 'exceptionalism' in order to separate its own behaviour from that permitted in the offline world while conventional economic models explain how the profit motive incentivises a race to the bottom where 'dark nudges' exploit vulnerability that harms individual users and imposes economic costs on society.

Philip W. S. Newall, 'Dark Nudges in Gambling', Addiction Theory and Research, Vol. 27, Issue 2, (2018), 65-67, accessed May 16, 2019, https://doi.org/10.1080/16066359.2018.1474206.

13. Connected toys and devices

No

14. Online tools

No

15. Data protection impact assessments

No

16. Governance and accountability

No

> The Lord Bishop of Gloucester has highlighted the damaging consequences of digital platforms absolving themselves of responsibility for access to content:

"The content we consume shapes how we see ourselves, other people and the world. It is no longer sufficient for social media and online platforms to cling to a simple dichotomy of platform versus publisher in order to escape responsibility for the content they promote and share. While previous generations' engagement with media might have been limited to print media and television broadcasts regulated by formal standards and watersheds, modern consumers, including children, are exposed to huge swathes of unregulated content. Research conducted by the UK Safer Internet Centre in 2016 found that more than 80 per cent of the teenagers surveyed had seen or heard online hate about a specific group."

The Lord Bishop of Gloucester, HL Deb January 11, 2019, vol 788 c376.

Q5. Do you think this standard gives rise to any unwarranted or unintended consequences?

1. **Best interests of the child**
No Rather, this draft Code is commendable for its principle of parity; reasserting the continuity of duty of care in both the online and offline 'worlds'. But this Code is also needed because Ofcom acknowledge that it is not possible simply to port existing legislation to cover the online world. This demonstrates the importance of establishing a principle-based code that is ethically robust while remaining technology-neutral. Ofcom report, Addressing Harmful Online Content, Sep. 2018, p4, accessed May 19, 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0022/120991/Addressing-harmful-online-content.pdf.
2. Age-appropriate application
No   Far from stifling innovation, the principle of 'safety by design' should stimulate Information Society Services (ISS) to innovate in lockstep with the needs of children. The precautionary principle recommending high privacy as the default unless there is 'compelling evidence' to justify the contrary, protects all children. The online world shares the offline world's ethical duty to differentiate between children and adults, and to respect and protect both the vulnerable and marginalised in the digital world. Moreover, the parable of the good Samaritan represents the call to practice ethically beneficial actions toward others that transcends both social and political jurisdictions The tech sector needs to accept the demands of responsibility above profitability and to acknowledge its own corporate social responsibility to uphold the common good. For greater clarification of these important issues, see appendix A (Attached separately).
3. Transparency
No
4. Detrimental use of data
No

5. Policies and community standards
No
6. Default settings
No
7. Data minimisation
No
8. Data sharing
No
9. Geolocation
No
10. Parental controls
No
11. Profiling
No
12. Nudge techniques
No   No; so long as care is taken to distinguish between beneficial and harmful nudging techniques. Some nudging, such as "time-out" prompts are likely to be beneficial, while there is now much evidence on the harmful consequenes of 'dark' or compulsive nudges like streaks and "near misses". While the draft code's DPIA template includes the question, "Does your service use any nudge techniques?" the draft is, again, short on both detail and examples of what constitutes nudging and what kinds of nudge are unnaceptable. This is significant because 'dark' nudges and 'sludge' (the practice of making commercially unwelcome features onerous to utilise) are already having tangible effects on the well-being of children. The 5Rights Foundation report, Disrupted Childhood, 2018, https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf.

13. Connected toys and devices
No

14. Online tools
No

15. Data protection impact assessments
No

 As noted above, while the draft code's DPIA template includes the question, "Does your service use any nudge techniques?" the draft is, again, short on both detail and examples. Dark nudges and 'sludge' (the practice of making commercially unwelcome features onerous to utilise) are already having tangible effects on the well-being of children.

The 5Rights Foundation report, Disrupted Childhood, 2018, accessed May 21, 2019, https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf. |
| **16. Governance and accountability** |
| No |

Q6. Do you envisage any feasibility challenges to online services delivering this standard?

1. **Best interests of the child**
No

Tailoring access to protect children's welfare while meeting their developmental needs is not technologically beyond the 'best interests' benchmark of the draft guidelines and should not be allowed to mask or defend poor practice. As the Bishop of Gloucester observes:
"The challenge for each of us is to ensure our language and our words validate every child as a whole person. How are we speaking to their inner being? Their character? This is about our encouragement and challenge of children, focusing on the heart of who they are so that they can continue to grow and flourish in becoming who God calls them to be." |

Rt Revd Rachel Treweek, Bishop of Gloucester, "From the Inside Out in an Upside Down World", accessed May 20, 2019, https://www.gloucester.anglican.org/wp-content/uploads/2018/04/cpc018_good_childhood_theology_web.pdf.
Indeed, as the 5Rights Foundation note: 'Innovation that doesn't respect the rights of children is not innovation – it's exploitation.' 5Rights Foundation, "5Rights welcomes the launch of the Information Commissioner's draft Age Appropriate Design Code", accessed May 20, 2019, https://5rightsfoundation.com/uploads/5rightsaadcbriefing.pdf.

2. Age-appropriate application

No

 Limiting content in an age-appropriate way depends upon robust mechanisms for verifying the user's age. Clearly, current solutions are not working and undermine trust in the tech sector.

Anthony Cuthbertson, "Snapchat admits its age verification system does not work", Independent Newspaper, May 19, 2019, accessed May 21, 2019, https://www.independent.co.uk/life-style/gadgets-and-tech/news/snapchat-age-verification-not-work-underage-ageid-a8829751.html.

The case for this draft Code's proportionate and risk-based approach to age-verification is overwhelming. Dilution of that principle would risk two consequences. First it would increase the difficulty of identifying the 'best interests' of individuals under 18 years of age accessing digital services. Secondly, dilution would diminish the commercial opportunities this provision invites for technological innovation in the digital world. Without a robust and rigorous age-verification mechanism, the duty of care principle that underpins these guidelines cannot be implemented.

3. Transparency

No

4. Detrimental use of data

No

5. Policies and community standards

No

 The defense of 'exceptionalism' to justify the disparity between policy and community standards in the online versus the offline world should be rejected. Under-18s comprise at least 20 per cent of UK internet users. The Church's own safeguarding policies affirm the belief that all human beings are created in God's image and that children fully deserve to be treated with dignity, care and compassion. These draft proposals are commendable for recognising the distinctive vulnerabilities and special needs of children and for upholding the United Nations Convention on the Rights of the Child. Children depend on all adults, not just on their own parents or primary care-givers, for both their physical safety and for their mental flourishing These guidelines materially contribute to realising the common good;
The principle of the common good, to which every aspect of social life must be related if it is to attain its fullest meaning, stems from the dignity, unity and equality of all people. […] The common good does not consist in the simple sum of the particular goods of each subject of a social entity. Belonging to everyone and to each person, it is and remains "common", because it is indivisible and because only together is it possible to attain it, increase it and safeguard its effectiveness, with regard also to the future.

6. Default settings

Yes

 Default settings need to be linked to age-verification far more effectively than current solutions permit. Far from stifling innovation, the principle of 'safety by design' should stimulate Information Society Services (ISS) to innovate in lockstep with the needs of children. The precautionary principle recommending high privacy as the default unless there is 'compelling evidence' to justify the contrary, protects all children. The online world shares the offline world's ethical duty to differentiate between children and adults, and to respect and protect both the vulnerable and marginalised in the digital world. Moreover, the parable of the good Samaritan represents the call to practice ethically beneficial actions toward others that transcends both social and political jurisdictions.

The tech sector needs to accept the demands of responsibility above profitability and to acknowledge its own corporate social responsibility to uphold the common good.
Tailoring access to protect children's welfare while meeting their developmental needs is not technologically beyond the 'best interests' benchmark of the draft guidelines and should not be allowed to mask or defend poor practice. As the Lord Bishop of Gloucester observes:
"The challenge for each of us is to ensure our language and our words validate every child as a whole person. How are we speaking to their inner being? Their character? This is about our encouragement and

challenge of children, focusing on the heart of who they are so that they can continue to grow and flourish in becoming who God calls them to be."

Rt Revd Rachel Treweek, Bishop of Gloucester, "From the Inside Out in an Upside Down World", accessed May 20, 2019, https://www.gloucester.anglican.org/wp-content/uploads/2018/04/cpc018_good_childhood_theology_web.pdf.

7. Data minimisation
No

8. Data sharing
No   Children's online activities should not be treated as mere 'behavioural surplus' for tech companies to use freely for commercial purposes. As the Lord Bishop of St. Albans has observed: "It has been encouraging that the Gambling Commission has taken a stronger line on an industry that in the past performed abysmally in its duty of care to its customers. If companies such as Facebook, Snapchat or YouTube are to behave, the regulators will need to have significant powers and there will need to be real independence. […] some cynics have been arguing that some of these companies simply budget in the fines as part of their ongoing business so that they can keep going as they have in the past. […] Therefore, there is a question about not only how we regulate them but how we get them to engage with the wider debate about the sort of world we want to create."   The Lord Bishop of St. Albans, HL Deb April 30, 2019, vol 797 c908-9.

9. Geolocation
No

10. Parental controls
No

11. Profiling
No

12. Nudge techniques
Yes

It is important to differentiate between beneficial and harmful nudges. Consequently, wider debate about the common good, and any attendant legislation, is essential because self-regulation has clearly failed. The tech industry appeals to 'exceptionalism' in order to separate its own behaviour from that permitted in the offline world while conventional economic models explain how the profit motive incentivises a race to the bottom where 'dark nudges' exploit vulnerability that harms individual users and imposes economic costs on society.

Philip W. S. Newall, 'Dark Nudges in Gambling', Addiction Theory and Research, Vol. 27, Issue 2, (2018), 65-67, accessed May 16, 2019, https://doi.org/10.1080/16066359.2018.1474206.

13. Connected toys and devices

No

14. Online tools

No

15. Data protection impact assessments

No

16. Governance and accountability

No
 The tech industry appeals to 'exceptionalism' in order to separate its own behaviour from that permitted in the offline world, but the Lord Bishop of Gloucester has highlighted the damaging consequences of digital platforms absolving themselves of responsibility for access to content:
"The content we consume shapes how we see ourselves, other people and the world. It is no longer sufficient for social media and online platforms to cling to a simple dichotomy of platform versus publisher in order to escape responsibility for the content they promote and share. While previous generations' engagement with media might have been limited to print media and television broadcasts regulated by formal standards and watersheds, modern consumers, including children, are exposed to huge swathes of unregulated content. Research conducted by the UK Safer Internet Centre in 2016 found that more than 80 per cent of the teenagers surveyed had seen or heard online hate about a specific group."

The Lord Bishop of Gloucester, HL Deb January 11, 2019, vol 788 c376.

Q7. Do you think this standard requires a transition period of any longer than 3 months after the code come into force?

1. **Best interests of the child**
No
2. Age-appropriate application
No
3. Transparency
No
4. Detrimental use of data
No
5. Policies and community standards
No
6. Default settings
No
7. Data minimisation
No
8. Data sharing

No

9. Geolocation

No

10. Parental controls

No

11. Profiling

No

12. Nudge techniques

No

13. Connected toys and devices

No

14. Online tools

No

15. Data protection impact assessments

No

16. Governance and accountability

No

Q8. Do you know of any online resources that you think could be usefully linked to from this section of the code?

1. **Best interests of the child**
Yes   UNICEF, United Nations Convention on the Rights of the Child, 1990 GDPR (Recital 38)

2. **Age-appropriate application**
No

3. **Transparency**
No

4. **Detrimental use of data**
No

5. **Policies and community standards**
No

6. **Default settings**
No

7. **Data minimisation**
No

8. **Data sharing**
No

9. **Geolocation**
No

10. Parental controls
No
11. Profiling
No
12. Nudge techniques
No
13. Connected toys and devices
No
14. Online tools
No
15. Data protection impact assessments
No
16. Governance and accountability
No

Q9. Is the 'Enforcement of this code' section clearly communicated?

Yes

Q10. Is the 'Glossary' section of the code clearly communicated?

Yes

Q11. Are there any key terms missing from the 'Glossary' section?

No

Q12. Is the 'Annex A: Age and developmental stages' section of the code clearly communicated?

Yes

Q13. Is there any information you think needs to be changed in the 'Annex A: Age and developmental stages' section of the code?

No

Q14. Do you know of any online resources that you think could be usefully linked to from the 'Annex A: Age and developmental stages' section of the code?

No

Q15. Is the 'Annex B: Lawful basis for processing' section of the code clearly communicated?

Yes

Q16. Is this **'Annex C: Data Protection Impact Assessments'** section of the code clearly communicated?

No

 While the draft code's DPIA template includes the question, "Does your service use any nudge techniques?" the draft is short on both detail and examples.

Q17. Do you think any issues raised by the code would benefit from further (post publication) work, research or innovation?

Yes

 More research is needed into 'nudging' with a view to distinguishing and differentiating between beneficial and harmful nudges, to help both industry and regulator establish and respect the boundary between both types of psychological nudge.

Age-verification is clearly not fit for purpose and more innovation is needed to establish a robust form of age-verification while also minimising data collection and data sharing.

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	☒
A body representing the views or interests of parents? Please specify: As Bishops in the Church of England we represent the interests of children, parents, church schools and parishioners of all ages.	☒
A child development expert? Please specify:	☐
An Academic? Please specify:	☐
An individual acting in another professional capacity? Please specify:	☐

A provider of an ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify:	☐
An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public or a parent)?	☐
An ICO employee?	☐
Other? Please specify: The Lord Bishop of Oxford, Rt Rev. Steven Croft The Lord Bishop of Chelmsford, Rt Rev Stephen Cottrell	☒

Thank you for responding to this consultation.

We value your input.