

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/NO.

If NO, then please provide your reasons for this view.

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

YES/NO.

If NO, then please provide your reasons for this view.

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/NO. If NO, then please provide your reasons for this view.
2. Age-appropriate application
YES/NO. If NO, then please provide your reasons for this view.
3. Transparency
YES/NO
4. Detrimental use of data
YES/NO. If NO, then please provide your reasons for this view.
5. Policies and community standards
YES/NO. If NO, then please provide your reasons for this view.
6. Default settings
YES/NO. If NO, then please provide your reasons for this view.
7. Data minimisation
YES/NO. If NO, then please provide your reasons for this view.
8. Data sharing
YES/NO. If NO, then please provide your reasons for this view.
9. Geolocation
YES/NO. If NO, then please provide your reasons for this view.
10. Parental controls

YES/NO.

If NO, then please provide your reasons for this view.

11. Profiling

YES/NO.

If NO, then please provide your reasons for this view.

12. Nudge techniques

YES/NO.

If NO, then please provide your reasons for this view.

13. Connected toys and devices

YES/NO.

If NO, then please provide your reasons for this view.

14. Online tools

YES/NO.

If NO, then please provide your reasons for this view.

15. Data protection impact assessments

YES/NO.

If NO, then please provide your reasons for this view.

16. Governance and accountability

YES/NO.

If NO, then please provide your reasons for this view.

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/NO.

If YES, then please provide details.

2. Age-appropriate application

YES/NO.

If YES, then please provide details.

3. Transparency

YES/NO.

If YES, then please provide details.

4. Detrimental use of data

YES/NO.

If YES, then please provide details.

5. Policies and community standards

YES/NO.

If YES, then please provide details.

6. Default settings:

YES/NO.

If YES, then please provide details.

7. Data minimisation

YES/NO.

If YES, then please provide details.

8. Data sharing

YES/NO.

If YES, then please provide details.

9. Geolocation

YES/NO.

If YES, then please provide details.

10. Parental controls

YES/NO.

If YES, then please provide details.

11. Profiling

YES/NO.

If YES, then please provide details.

12. Nudge techniques

YES/NO.

If YES, then please provide details.

13. Connected toys and devices

YES/NO.

If YES, then please provide details.

14. Online tools

YES/NO.

If YES, then please provide details.

15. Data protection impact assessments

YES/NO.

If YES, then please provide details.

16. Governance and accountability

YES/NO.

If YES, then please provide details.

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

1. Best interests of the child

YES/NO.

If YES, then please provide your reasons for this view.

2. Age-appropriate application

Yes

Age-appropriate application obligations mean that many ISS will likely introduce age-verification measures, for the reasons described in our response to Q 7.2.

With age-verification technologies not yet effective at the accuracy levels implied by the code, ISS will have to introduce analogue measures or innovate develop their own interventions.

For smaller ISS, the costs and burden to the business of taking either of these actions may be prohibitively expensive, or at the very least take up a greater proportion of revenue relative to larger established ISS.

Age-verification obligations may therefore impact on digital competition and entrench the dominance of current multinational large-scale ISS who have the resources to comply with them.

The GDPR's one-stop shop provision also means some large ISS may be able to switch their lead supervisory authority to a body in the EU outside

of the UK where the code will not apply. This would give a further competitive advantage to multinationals ISS over British start-ups and SME ISS.

The ICO should carefully consider how to mitigate these competition risks, for example incentivising large ISS to share age-verification technologies and innovations with smaller ISS.

3. Transparency

Yes

The code states that “depending upon the age of the child, you should also prompt them to speak to an adult before they activate any new use of their data, and not to proceed if they are uncertain”. Relying on adults to provide guidance to children is however problematic on several fronts:

1. The UK Council for Internet Safety's "Children's Online activities, risks and safety" research has found children can be reluctant to speak to adults regarding their use of ISS for fear of embarrassment, punishment and losing access to device and services

2. Doteveryone's "People, Power and Technology" research finds adults lack the digital understanding needed to navigate the privacy trade-offs of consent, and make fully informed decisions around the data benefits & risks to their child - 45% of survey respondents don't realise adverts can be targeted based on previous online behaviour and 42% would like to do more change their privacy settings but don't know how. More than two-thirds (70%) are unaware free-to-use apps make money from user data, with this figure dropping to 62% for social media and 57% for search engines.

3. Ofcom and ICO's recent "Online Nation" research paints a similar picture: 69% of adults surveyed accept terms and conditions without reading them. 46% don't know how search engines are funded.

4. New research from Which found that, a year after its introduction, a third of people was unaware of GDPR and that their data rights had changed. And one third who knew there has been a change, weren't confident what extra protections they now had.

5. Adult's “first-order preferences” - preferences and choices made in the moment that determine actions, often impulsively - will likely differ from their “second-order preferences” - choices made on reflection, generally separated from immediate temptations. The Behavioural Insights Team's "The behavioural science of online harm and manipulation, and what to

do about it" research has found that online markets and online consent rely on "far more fluid expressions of first order, impulsive preferences".

At the point of consent, adults are likely to be guided by first-order preferences and influenced by the pressures present at the time. Several contextual factors - including the desire to occupy and entertain their child, a lack of time to fully consider implications of consent, desire to avoid a confrontation with their child and/or partner and an inability to explain their decision in the moment - mean these pressures are, on balance, likely to encourage rather than discourage adults to unduly give consent.

6. ISS providers may find it difficult to verify whether this conversation between child and adult has taken place - a tick-box will not be adequate as children can easily circumvent this. Measures such as adults providing age-verification before providing secondary consent may be required.

4. Detrimental use of data

YES/NO.

If YES, then please provide your reasons for this view.

5. Policies and community standards

YES/NO.

If YES, then please provide your reasons for this view.

6. Default settings

YES/NO.

If YES, then please provide your reasons for this view.

7. Data minimisation

YES/NO.

If YES, then please provide your reasons for this view.

8. Data sharing

YES/NO.

If YES, then please provide your reasons for this view.

9. Geolocation

YES/NO.

If YES, then please provide your reasons for this view.

10. Parental controls

YES/NO.

If YES, then please provide your reasons for this view.

11. Profiling

YES/NO.

If YES, then please provide your reasons for this view.

12. Nudge techniques

YES/NO.

If YES, then please provide your reasons for this view.

13. Connected toys and devices

YES/NO.

If YES, then please provide your reasons for this view.

14. Online tools

YES/NO.

If YES, then please provide your reasons for this view.

15. Data protection impact assessments

YES/NO.

If YES, then please provide your reasons for this view.

16. Governance and accountability

YES/NO.

If YES, then please provide your reasons for this view.

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

1. Best interests of the child

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

2. Age-appropriate application

Yes

Please see response to Q7.2

3. Transparency

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

4. Detrimental use of data

Yes

The code states that to meet the standard regarding detrimental use of data, ISS "should also keep up to date with Government advice on the welfare of children in the context of digital or online services...you should not process children's personal data in ways that have been formally identified as requiring further research or evidence to establish whether or not they are detrimental to the health and wellbeing of children". We believe that the government is not currently able to provide adequate advice in this area.

Doteveryone's Regulating for Responsible Technology research into the UK's regulatory system (Reference: <https://doteveryone.org.uk/project/regulating-for-responsible-technology/>) has found that the evidence-base regarding online harms and detrimental use of data is lacking.

A lack of rigorous evidence around online harms has also been identified by others, with the issue of screen time a microcosm of the wider problem. A group of over 100 researchers in the Children's Screen Time Action Network – working in technology, psychology and other fields – have noted in an open letter to the American Pediatricians Association, that "the public discourse around the effects of screen time and technology use are being marred by the use of emotionally evocative language, scaremongering, and a general lack of solid, open and reproducible evidence" (Reference: <https://screentimenetwork.org/apa>). A February 2019 review by the Chief Medical Officer (CMO) of the impact of screentime on mental health found "we do not have clear evidence [of a causal relationship between screenbased activities and mental health problems]...an association has been seen between those who engage in screen-based activities more frequently and/or over longer periods, and mental health problems. However, it is not clear that the screen-based activities are the cause of those problems." (Reference: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf)

Against this backdrop of uncertainty and mixed evidence, the need for a single, authoritative body to give independent advice to ISS is particularly acute.

The CMO, ICO, Cabinet Office, Department for Digital Culture, Media and Sport, UKRI and UKCIS could all conceivably play a role in developing this evidence-base and providing advice around the detrimental use of data. There is an urgent need to define how responsibilities between these bodies should be shared, and for the government to invest in developing the evidence-base around online harms and detrimental use of data on an ongoing basis.

As the body responsible for providing guidance on other aspects of the code, we recommend that the ICO hold primary responsibility for issuing advice around the detrimental impacts of data use as part of a wider one-stop-shop advice function. This advice should include regular bulletins of relevant evidence that ISS can subscribe to.

The ICO should also lead the development of a coherent long-term strategy for developing the evidence-base around detrimental use of data with the organisations mentioned above.

5. Policies and community standards

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

6. Default settings

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

7. Data minimisation

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

8. Data sharing

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

9. Geolocation

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

10. Parental controls

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

11. Profiling

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

12. Nudge techniques

Yes

The application of "nudge techniques" is an important but ambiguous area. Clear lines will need to be drawn between practices that drive necessary engagement and manipulative nudging, and ISS will likely need support to interpret the code in this area.

We recommend that the ICO look to establish a library of design patterns and standards that organisations to design responsible nudge-free services. They should also maintain an open directory of case studies where companies have been found guilty of using nudge techniques, and explore ways for users to report the use of unfair nudging practices to the ICO.

The ICO should also explore ways to stimulate the open source development of responsible design patterns - for example through consultation, a series of grants for civil society organisations or design challenge prizes.

13. Connected toys and devices

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

14. Online tools

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

15. Data protection impact assessments

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

16. Governance and accountability

Yes

The government's Online Harms White Paper will place a duty of care on digital services to protect users from online harm. Where these harms relate to content uploaded, shared between and created by users, some level of general monitoring of content is likely to be required of ISS to fulfill the White Paper's obligations to "anticipate emerging harms" and proactively identify harmful content.

These obligations may be in tension with the Age-appropriate Design Code's principles of data minimisation and threaten children's rights to freedom of speech and privacy.

The ICO and government should therefore provide further guidance to companies around how these obligations affect each other, and set out best practice guidance in meeting both these obligations - In particular further clarification around what constitutes a "compelling reason" for data gathering in relation to safeguarding.

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

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

2. Age-appropriate application

Yes

The GDPR allows countries within the European Union to set age thresholds for defining who constitutes and adult in regards to consent, which range from 16 years in France to 13 in UK. ISS services who wish to engage in data gathering that breaches the code for adult users will also be required to introduce age-verification measures.

These drivers mean there will likely be a significant uptake of age-verification services by ISS following the introduction of the code.

Current age-verification policies and processes are not adequate: Most social media sites including Facebook, Twitter, Instagram and Snapchat have a minimum age requirement of 13, but research by Ofcom finds 21% of 10-year-olds, 34% of 11-year-olds and 48% of 12-year-olds say they have at least one profile on social media. (Reference: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf)

The Code states that ISS "must be able to demonstrate that children cannot easily circumvent the age checks", meaning new policies and technologies must be introduced. Yoti's industry leading automated age-verification technology is however only accurate to within 3 years. (Reference: https://s3-eu-west-1.amazonaws.com/prod.marketing.asset.imgs/yoti-website/Yoti-Age-Scan_Digital.pdf)

This means that large ISS looking to introduce age-verification measures that meet the obligations of the code must either wait for existing technology to improve accuracy levels, develop technology that is significantly more effective than current solutions or introduce non-automated technological processes on a scale that can cope with millions or billions of users. None of these options are feasible on a timescale of 3 months.

The British Board of Film Classification will from July be responsible for overseeing the age-verification of porn viewers in the UK. Civil society organisations including Open Rights Group have commented that "The BBFC's draft guidance [on age-verification] lacked even the basic privacy protections required for other digital tools like credit card payments and email services". These comments suggest that other regulatory approaches to age-verification are not yet effective enough to be adopted by the ICO once the code is in force.

We welcome the Commissioner's commitment to lead the development of technical standards, auditing and certification of age-verification technologies. We recommend the ICO also:

1. Audit large ISS' non-technological measures for age-verification processes to ensure adequacy
2. Establish a cross-regulatory working group on age-verification including, for example the BBFC, alcohol & gambling oversight bodies

3. Develop incentives (or regulatory obligations if required) for ISS to share effective age-verification innovations with other ISS.

3. Transparency

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

4. Detrimental use of data

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

5. Policies and community standards

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

6. Default settings

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

7. Data minimisation

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

8. Data sharing

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

9. Geolocation

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

10. Parental controls

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

11. Profiling

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

12. Nudge techniques

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

13. Connected toys and devices

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

14. Online tools

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

15. Data protection impact assessments

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

16. Governance and accountability

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

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/NO.

If YES, then please provide details (including links).

2. Age-appropriate application

YES/NO.

If YES, then please provide details (including links).

3. Transparency

YES/NO.

If YES, then please provide details (including links).

4. Detrimental use of data

YES/NO.

If YES, then please provide details (including links).

5. Policies and community standards

YES/NO.

If YES, then please provide details (including links).

6. Default settings

YES/NO.

If YES, then please provide details (including links).

7. Data minimisation

YES/NO.

If YES, then please provide details (including links).

8. Data sharing

YES/NO.

If YES, then please provide details (including links).

9. Geolocation

YES/NO.

If YES, then please provide details (including links).

10. Parental controls

YES/NO.

If YES, then please provide details (including links).

11. Profiling

YES/NO.

If YES, then please provide details (including links).

12. Nudge techniques

Yes

If YES, then please provide details (including links).

13. Connected toys and devices

No

If YES, then please provide details (including links).

14. Online tools

YES/NO.

If YES, then please provide details (including links).

15. Data protection impact assessments

Yes

Doteveryone's TechTransformed tools can be used by the developers and owners to map and mitigate future unintended consequences of their products and services: <https://www.tech-transformed.org/>

DPIA's should not be seen by ISS as mere compliance exercises. They are an opportunity to spot risks to individuals, communities and different demographics, and should be a comprehensive exercise considering the economic, social, ecological and political consequences of data gathering and use. TechTransformed is designed to help ISS consider these broad range of factors. We hope that integrating TechTransformed into the DPIA process will mean the Age Appropriate Design Code has a broader impact on improving technology for all users.

16. Governance and accountability

YES/NO.

If YES, then please provide details (including links).

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

YES/NO.

If NO, then please provide your reasons for this view.

To ensure the widespread adoption of best practice in the industry it is important that enforcement actions are accompanied by communications to other organisations to share learning. Experience from other sectors (eg improvement in safety in the chemicals industry) points to the role peer learning can play in driving up standards.

Therefore enforcement actions must include clear 'lessons learned' information. Over time this can support the development of a design pattern library as described above.

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

YES/NO.

If NO, then please provide your reasons for this view.

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

YES/NO.

If YES, then please provide your reasons for this view.

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

YES/NO.

If NO, then please provide your reasons for this view.

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

YES/NO.

If YES, then please provide your reasons for this view.

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?

YES/NO.

If YES, then please provide details (including links).

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

YES/NO.

If NO, then please provide your reasons for this view.

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

YES/NO.

If NO, then please provide your reasons for this view.

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

Yes

The code states that consent for certain age groups "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 upon written communications". It stops short of specifying what this imagery might look like, what it needs to communicate and where it should be used. ISS will be free to develop their own approaches when the code comes into force.

Keeping up with the complexity and pace of digital change is already a massive challenge for children and parents (as evidenced by our response to Q3.3). Whilst the introduction of visual iconography is intended to make understanding terms and conditions easier, there is a risk that they may ultimately increase the cognitive burden on people if each ISS develops their own visual languages for terms and conditions - and regularly updates and changes them as their products and policies evolve.

Without clear standards, testing and certification, iconography and gamification may be used to nudge people into consenting.

To mitigate these risks, there is a need to develop a common, universally recognised standard for visual language used in online consent. The success of standardised visual iconography in other sectors including Health and Safety shows the merits of this approach. (Reference: <https://www.osha.gov/dsg/hazcom/hc2inf2.html>)

The ICO should lead on the development of this standardisation. Doteveryone recommends the ICO should do so by:

1. Conducting user research with children and parents to develop a rigorous taxonomy of consent & privacy - identifying which aspects (for example when their data is being shared with a third party, when data stored to a certain level of security, if data will be used to target/personalise content) of consent are currently less understood, and which are a priority to be aware of.
2. Hosting a design competition for external organisations to propose visual iconographies to communicate the taxonomy developed in stage 1.
3. Convening policymakers, regulators, standards organisations, ISS, civil society and childrens groups to work towards adopting a common standard for visual language and consent.

A similar approach should also be applied to develop a standardised visual iconography for online reporting tools described in section 14 of the code, and for notifying children when their geolocation is being tracked.

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	<input type="checkbox"/>
A body representing the views or interests of parents? Please specify:	<input type="checkbox"/>
A child development expert? Please specify:	<input type="checkbox"/>

<p>An Academic?</p> <p>Please specify:</p>	<input type="checkbox"/>
<p>An individual acting in another professional capacity?</p> <p>Please specify:</p>	<input type="checkbox"/>
<p>A provider of an ISS likely to be accessed by children?</p> <p>Please specify:</p>	<input type="checkbox"/>
<p>A trade association representing ISS providers?</p> <p>Please specify:</p>	<input type="checkbox"/>
<p>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)?</p>	<input type="checkbox"/>
<p>An ICO employee?</p>	<input type="checkbox"/>
<p>Other?</p> <p>Please specify:</p> <p>Doteveryone - an independent non-profit think-tank</p>	<input checked="" type="checkbox"/>

Thank you for responding to this consultation.

We value your input.