

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?

No

It is clear in nearly all respects but for retailers there is an element of lack of clarity. In 'who is this code for' it states it applies to you 'if you provide online products or services (including....connected toys or devices) that process personal data and are likely to be accessed by children in the UK'. Later it provides a list of the rights of the child that it seeks to protect. From this introduction it could appear that the code ONLY applies to the sale of connected toys whereas later in the document it would seem to have more extensive applicability. It would be useful to make this clear (if indeed it is the case that it is more extensive) in the introduction for the sake of those who may not read further if they think it does not apply to them.

It would also be useful to have some guidance on how this Code will interact and coordinate with the upcoming Guidance on Children and the GDPR given that one covers ISS likely to be accessed by children while the other covers ISS that offer services to children.

Also the interaction with the IoT initiative and the Online Harms proposals could be spelt out.

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

No

Not entirely. There are references to marketplaces and the sale of goods - and to the application to small businesses 'only if you sell your products online'. However, these are all mentioned only in passing with most of the text being about services that are provided and completed online. It might be clearer if the sentence 'the focus of the code is to set a benchmark for the appropriate protection of children's personal data' appeared right at the beginning of the section to provide a context for the rest. It is not entirely clear from the list of the rights of the child how a seller of legal goods could be affected. Therefore it would be helpful to have a bit more explanation in a separate section on this particular aspect and how it might apply, not least given that children often cannot make a purchase in their own right. A subsection entitled 'sale of goods' would be helpful. It would also be helpful if there were clarification of the responsibilities of marketplaces for traders on their sites beyond the actual material on the marketplace site. In our view the individual trader should be responsible for his use of any data he gathers and this should be clear - as should whether this applies to a consumer selling on the site.

In addition further explanation of the meaning of 'likely to' be accessed would be useful and the key criteria that a provider might apply to an assessment, perhaps even with examples of where the borderline might be. An explanation was provided on request by an ICO official who said - 'It refers to likelihood of 'prejudice' occurring but our intention is to use the same threshold for likely to be accessed by. So there would have to be a very significant chance of children accessing the service, but the chance of them doing so wouldn't have to be more probable than not.

'Would be likely' refers to a lower level of probability than 'would', but one which is still significant. This interpretation is based on the judgment of Mr Justice Munby in R (on the application of Lord) v Secretary of State for the Home Office [2003] EWHC 2073 (Admin) (a Data Protection Act case) who said:

"Likely connotes a degree of probability that there is a very significant and weighty chance of prejudice to the identified public interests. The degree of risk must be such that there 'may very well' be prejudice to those interests, even if the risk falls short of being more probable than not." (paragraph 100). Hints at how to make an objective assessment of this would be helpful and also the relationship between likelihood of access and lack of likelihood of causing detriment and where the balance might lie if both likelihood of access is small and likelihood of detriment is small.

Third, we understand from discussions with ICO officials that social media sites such as Facebook are responsible for application of the Code on their sites and thus a retailer would only be responsible for its facebook page to the extent that it used data from its facebook page. This should be made clear and it should not be possible for social media sites to absolve themselves of responsibility by terms and conditions.

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
The section is clear as far as it goes - but it is not immediately apparent how these interests apply in practice to the sale of goods.
2. Age-appropriate application
No

The box right at the beginning has resulted in some newspapers suggesting that all websites must have age verification measures in place or you must apply the standards in the code to all users - whereas ICO officials have suggested to us that a DPIA type process might be applied whereby a website owner asks first whether the site is likely to be accessed by children and then if the answer is that it is, the second question is are their interests likely to be affected adversely. If this is correct, the headline box could lead to confusion. This is also linked to the need for a better explanation of how a website that sells legal goods is likely to be affected - and hence the request for a separate explanation earlier.

We also note the paragraphs on age verification options. The government has failed to provide a robust standard against which providers on online age verification can be audited. We therefore welcome the statement that the Commissioner will support work to establish clear industry standards and certification schemes to assist...in identifying robust age verification systems which comply with data protection standards'.

3. Transparency

Yes

It is clear but whether a child is likely to read it is far less certain. In the case of a retail website selling goods, the child is more likely to be interested in the product than reading explanations - as we know from the lack of attention by all users to statements of terms and conditions.

4. Detrimental use of data

Yes

It is clear but it is important that the code should add to rather than duplicate other legal requirements or codes such as the CAP Code of the ASA.

5. Policies and community standards

Yes

A rather long way of saying - do what you say you do!

6. Default settings

Yes

As stated - most of the examples here and elsewhere seem relevant to the provision of services online rather than the sale of goods. This suggests a section bringing everything together for sale of goods websites would be really helpful.

7. Data minimisation

Yes

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

8. Data sharing

Yes

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

9. Geolocation

Yes

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

10. Parental controls

Yes

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

11. Profiling

Yes

However it would be helpful to have an example from the sale of a toy, for example - with an indication of the acceptability or otherwise of leading the child to look at another similar toy.

12. Nudge techniques

Yes

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

13. Connected toys and devices

No

This is an important piece of advice and needs to be totally clear. The initial box refers to 'providing' a connected toy or device. Does this mean selling such a toy or device or selling such a toy or device and providing the network/servers over which it will operate - which may well be provided by an external party and require a subscription or use of the home wifi.

The advice in the code is not clear. It does not really deal with the sale of a toy or device where this is the sole act of the retailer. It says that 'outsourcing' the connected element to someone else does not absolve you of responsibility but it does not deal with the sale of a toy without any further service provision which is then the responsibility of the consumer. (The IoT dcms consultation deals with potential labelling for whether a device is security compliant but this is not consistent with the code statement relating to 'when you are making sure the product incorporates adequate security measures to mitigate risks....The two need

to be brought into line as the DCMS regulation preferred outcome seems to be a label that states whether or not the device is security compliant not that it is).

Thus there needs to be clarity on the meaning of 'provide' and this should be a legal definition of what happens in the sale of goods and services; and the section on outsourcing the 'connected' element needs to be clarified for a situation where no such outsourcing is supplied by the retailer. Is it a responsibility of the manufacturer if he provides the server - and what if the manufacturer is in China? How can this be enforced? Does the retailer have a responsibility in terms of the contract with the manufacturer? What about direct imports by consumers?

The section on providing clear information about your use of personal data at point of purchase and on set-up suggests using an icon and other matters of detail. This needs to be joined up with the DCMS consultation on IoT products not least on the use of icons. We cannot have two differing requirements in two sets of legal rules.

14. Online tools

Yes

But somewhat unrealistic in terms of what a child might do. It is also well known that excessive use of icons can be counter-productive not least if the icons are not universal.

15. Data protection impact assessments

Yes

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

16. Governance and accountability

Yes

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

No

If YES, then please provide details.

2. Age-appropriate application

No

If YES, then please provide details.

3. Transparency

No

If YES, then please provide details.

4. Detrimental use of data

No

If YES, then please provide details.

5. Policies and community standards

No

If YES, then please provide details.

6. Default settings:

No

If YES, then please provide details.

7. Data minimisation

No

If YES, then please provide details.

8. Data sharing

No

If YES, then please provide details.

9. Geolocation

No

If YES, then please provide details.

10. Parental controls

No

If YES, then please provide details.

11. Profiling

No

If YES, then please provide details.

12. Nudge techniques

No

If YES, then please provide details.

13. Connected toys and devices

No

If YES, then please provide details.

14. Online tools

No

If YES, then please provide details.

15. Data protection impact assessments

No

If YES, then please provide details.

16. Governance and accountability

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

No

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

2. Age-appropriate application

Yes

lack of clarity on when age verification systems should be used can lead to unintended expectations among the media.

3. Transparency

Yes

Excessive provision of information can lead to consumers ignoring important elements, not least when combined with Terms and conditions information. Consideration should be given to developing a short list of key requirements.

4. Detrimental use of data

No

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

5. Policies and community standards

Yes

It should be made clear which have precedence - this code or the other standards This is really an information section and it should be clearer which pieces of information are new and only in this code.

6. Default settings

Yes

Excessive need to change multiple settings where a child may be an occasional user (such as a visitor) may lead to lack of compliance at the user end.

7. Data minimisation

No

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

8. Data sharing

No

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

9. Geolocation

No

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

10. Parental controls

No

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

11. Profiling

Yes

Potential for confusion between the profiling of the child and that of the adult using the same website for sale of goods - or even the adult buying the goods for the child at the child's instigation.

12. Nudge techniques

No

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

13. Connected toys and devices

Yes

In as much as it is not totally clear in all circumstances who this is addressed to (ie where the sale is only of the toy or device and nothing more or where the sale is on a marketplace). Potential for differing requirements with DCMS regulation.

14. Online tools

No

If YES, then please provide your reasons for this view.
15. Data protection impact assessments
No
If YES, then please provide your reasons for this view.
16. Governance and accountability
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
In distinguishing between the need to protect the health and wellbeing of the child under this code and the health requirements both voluntary and mandatory.
2. Age-appropriate application
Yes
In identifying when to use age verification for the whole website as opposed to sale of certain products and in lack of recognised online age verification standards -and deciding whether access to a website with age restricted products is a problem for the code even if under age children cannot make a purchase
3. Transparency
Yes
presenting all the information requirements of the code and other t and c in a way that they even stand a chance of being read - not least by children
4. Detrimental use of data
No
If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
5. Policies and community standards
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

Making the options clear to all

7. Data minimisation

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

No

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

9. Geolocation

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

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

ensuring legitimate profiling of a purchaser of goods on the site is distinguished from profiling of a child on the site

12. Nudge techniques

Yes

knowing when a child is on the site rather than an adult.

13. Connected toys and devices

Yes

making it clear to the user who is responsible for what aspects

14. Online tools

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

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

No

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

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

The code should come into effect as a whole not in stages. It takes more than 3 months to adapt a website with some aspects taking longer than others. It might be possible to distinguish between the aspects that require a website to be adapted compared with others that do not in which case it may be possible to imagine a 2 stage transition. There are in particular elements applicable to the IoT which require information to be given with the product or online - and where there will be products on the shelf or need for liaison with manufacturers if icons are to be used. DCMS is looking at 2 years for its labelling changes, for example. As a rule where a website or data gathering needs change, then at least 6 months is required.

2. Age-appropriate application

Yes

adaptation of website if necessary

3. Transparency

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

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

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

adaptation of website

7. Data minimisation

Yes

adaptation of website.

8. Data sharing

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

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

testing information for understanding by ranges of children and adaptation of website

11. Profiling

Yes

if necessary to adapt website to distinguish between child and adult.

12. Nudge techniques

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

to get measures in place to meet requirements for information, making any adjustments to service contracts, getting manufacturers to change information, get icons developed - up to 18 months

14. Online tools

Yes

adaptation of website.

15. Data protection impact assessments

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

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

No

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

2. Age-appropriate application

No

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

3. Transparency

No

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

4. Detrimental use of data

No

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

5. Policies and community standards

No

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

6. Default settings

No

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

7. Data minimisation

No

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

8. Data sharing

No

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

9. Geolocation

No

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

10. Parental controls

No

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

11. Profiling

No

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

12. Nudge techniques

No

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

13. Connected toys and devices

Yes

dcms and international codes.

14. Online tools

YES/NO.

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

15. Data protection impact assessments

No

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

16. Governance and accountability

No

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

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

Yes

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

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

Yes

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

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

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

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?

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?

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

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

But it would be useful if the DPIA guidance and template had clear guidance on how to assess whether an online service is an ISS likely to be accessed by children - ie what are the key questions to ask and to whom

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

Yes

as indicated the application to sale of goods

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"/>
An Academic? Please specify:	<input type="checkbox"/>

<p>An individual acting in another professional capacity? Please specify:</p>	<input type="checkbox"/>
<p>A provider of an ISS likely to be accessed by children? Please specify:</p>	<input type="checkbox"/>
<p>A trade association representing ISS providers? Please specify: British Retail Consortium (BRC) the lead trade body representing online and offline retailers and omnichannel.</p>	<input checked="" 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? Please specify:</p>	<input type="checkbox"/>

Thank you for responding to this consultation.

We value your input.