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?

No

Who is the code for? This section states that the code applies to online services or products that process personal data and are likely to be accessed by children. This section needs further explanation and examples of the evidence required to demonstrate that a child is not likely to access the service. The US Children's Online Privacy Protection Act (COPPA) defines audiences into the following categories, primary child directed, child directed mixed audience and general audience which can help clarify the service provider's intention. However, many general audience services that target users 13 and older have actual knowledge that children are accessing their services. PRIVO recommends that a service should specify the target audience and age range and provide documented evidence that children are not accessing it if they are not targeting a 12 years or younger audience. A service should be able to provide composite audience information if data

subject's ages are screened or collected and supporting documentation to show the target age range.
PRIVO recommends that the Code includes clear defintion of audiences including mixed.

## 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<br><br>If NO, then please provide your reasons for this view. |
| **2. Age-appropriate application** |
| YES/NO.<br><br>PRIVO welcomes the recognition of the need to verify age. Self selecting age has led to children "ageing up" and circumventing age gates to access services content that can result in risks and harms. The Code calls on services to "tailor measures" in the code for the age of the users if the ISS is not verifying age. PRIVO recommends clear guidance on when an ISS should verify age and when it can rely on self declaration according to the risk. Therefore a social media platform should need to verify age as profiling and public sharing of personal data is a core activity of the service but a game that only collects non personal data such as an anonymous display or username and a password and moderates to ensure personal data is not shared can tailor measures in the code to the age of the user. Age verification and other methods to establish age in the light of available technology are available and could be regularly evaluated and added to an approved list of methods published under the Code. PRIVO also recommends an ISS should declare the age of its intended audience. |
| **3. Transparency** |

YES/NO

PRIVO welcomes the inclusion of transparency in the Code and the examples of how to communicate information to a child. PRIVO recommends that the Code be more explicit about what types of processing activity the ISS needs to provide transparent information on and that this information must be understandable to the ages of the child using the service. For example, a child is unlikley to understand the following commonly used language: we share your personal information with third parties. Instead it should state: we share your personal information with other people and go on to explain what is shared and why.The Code could provide key examples of language that the Information Commissioner would expect to see.

**4. Detrimental use of data**

No

The inclusion of the issue of detrimental use of a child's data is vital. Children are not likely to understand the implications of what happens to their personal data. PRIVO works with hundreds of ISSs and believes that the detrimental use of data needs to be defined further. PRIVO recommends the Code is more explicit on the defintion. For example, interest based advertising results in profile building and remarketing and pushes a child in a certain direction.Both practices are detrimental to a child.

**5. Policies and community standards**

Yes

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

**6. Default settings**

No

The inclusion of high privacy by default settings is both vital and welcome. Some of the big tech giants/social media platforms have launched privacy settings to meet standards but these settings are often easy to change and the consequences are not clear and transparent to the user. PRIVO recommends that the Code is clearer with regard to additional measures put in place when a child attempts to change a setting.

**7. Data minimisation**

Yes

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

**8. Data sharing**

No

Data sharing needs to be considered in all its guises. Sharing of a persistent identifier to track a child and tailor their experience without their knowledge is common among ISSs today. PRIVO recommends that the Code is explicit with regard to tracking children's behavior online to build a profile of them in order to push products or present specific content. For example, apps publishers use attribtuion and install tracking for business purposes but this process collects identifiers of child users and tracks them without any awareness from the data subject children, minor or adult. Explicitly citing the sharing of persistent identifers as data sharing that poses risks and harms will reinforce the transparency principle and support the "education" in terms of what is detrimental data.

**9. Geolocation**

No

PRIVO recommends that precise geolocation data that is shared should require the consent of the holder of parental responsibility. A child may not understand the risks inherent in sharing this data.

**10. Parental controls**

Yes

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

**11. Profiling**

No

PRIVO recommends that the Code makes it explicitly clear that profiling for personalised advertising, remarketing and targeting should be prohibited. It is not in the best interests of the child. The Code is not clear on this matter. A clear distinction between contextual advertising and interest based advertising is required. Contextual advertising allows the child to see content that interests them as an aggregated and anonymised group and does not track the child or build a profile of their behaviour. Therefore contextual advertising is appropriate for children.

**12. Nudge techniques**

Yes

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

**13. Connected toys and devices**

No

The Code should set a minimum standard of security for connected devices that process a child's personal data. Industry also requires clear guidance on what constitutes a connected device.

**14. Online tools**

Yes

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

**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**

Yes

COPPA clearly defines audiences which assists ISSs to apply appropriate measures. A primary child directed treats all users as children, mixed audience can restrict the experience for u13 users by screening with a compliant neutral age gate, general audience blocks users u13 from the experience. The mixed audience approach meets a common need in the online world. COPPA allows for a compliant neutral age screen to restrict the experience for younger users without blocking them from an ISS that they maybe attracted to. The gate can screen to restrict or to collect parent consent if consent is the lawful basis for processing. Important points to note: the mixed audience approach should not require that the majority of users are 13 and older and the ISS only attracts a few younger users as there is a demand to apply this audience definition for an ISS that may for example have a 50/50 split in the age of the audience, 50% u13 and 50% 013. PRIVO recommends consideration of the audience definitions and that an ISS should declare their target audience publicly in their notices and terms.

**3. Transparency**

YES/NO.

If YES, then please provide details.

**4. Detrimental use of data**

No

**5. Policies and community standards**

Yes

PRIVO recommends use of software coupled with human review to support user behavior policies. This approach has been tried and tested in many ISSs multi player games for example and can help promote appropriate behavior and minimise risks. There are two leading companies that provide software in this field.

**6. Default settings:**

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

The approach has been demonstarted as best practice in some ISS and in the existing PRIVO iD Platform (a consent and identity management platform). See supporting document.

**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** |
| No<br><br>If YES, then please provide details. |
| **14. Online tools** |
| No<br><br>If YES, then please provide details. |
| **15. Data protection impact assessments** |
| No<br><br>If YES, then please provide details. |
| **16. Governance and accountability** |
| Yes<br><br>Certification schemes will support accountability and governance once launched. An example of the success of such schemes in the area of child privacy are the FTC approved COPPA safe harbor programs which have demonstrated ISSs compliance with the US regulation for over a decade. |

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

| |
|---|
| 1. **Best interests of the child** |
| No<br><br>If YES, then please provide your reasons for this view. |
| **2. Age-appropriate application** |
| Yes<br><br>Defining the age of the audience and declaring intended target age group is key to preventing misinterpretation of "likely to attract children". PRIVO recommends audience definitions with explicit guidance on when to use age verification versus age screen. This will help to ensure that ISSs with child users can no longer "turn a blind eye" to the real age of users which results in risks to the child particularly on social media sites. |
| **3. Transparency** |
| No |

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

**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

The Code does not clearly explain when or if profiling for advertising and marketing is acceptable. The misuse of persistent identifiers for advertisting, remarketing and attribution has consequences for children. These practices are at the core of most revenue models unless the ISS is compliant with the US COPPA.

**9. Geolocation**

Yes

Collection and or sharing of precise location data by a controller puts a child at risk. The Code is not explicit on this subject and this could lead to an interpretation by an ISS that has consequences for a child.

**10. Parental controls**

YES/NO.

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

**11. Profiling**

Yes

Unless there is clarification on this point as it relates to advertising and marketing there is room for ISSs to continue to track children and personalise their online experience, buidling a profile of them and skewing their experience for commercial purposes with disregard for the best interests of the child.

**12. Nudge techniques**

YES/NO.

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

**13. Connected toys and devices**

Yes

A minimum standard should be set for security and privacy related to connected devices. If not the consequences will be differing standards and no level playing field for big business, medium and start ups.

**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**

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**

No

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

**3. Transparency**

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**

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**

Yes

Cost may prove an issues for some ISSs that need to manage communities at a more granular level if they are to implement measures to prevent user behavior infringing the Code.

**6. Default settings**

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**

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**

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**

No

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

**13. Connected toys and devices**

Yes

Some connected devices may need to implement security measures not currenty in place which could take time and incurr costs. A timeframe may need to be agreed that is longer than any transition period so far discussed.

| |
|---|
| **14. Online tools** |
| No<br>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<br>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<br>For ISSs that have built their services withouth privacy by design and default baked in, the Code requires a rebuild. A timeline should be agreed for the transition process for any ISSs that need to rebuild its service. This is a time and resource intense process and has cost implications, so a case by case basis may need to be considered. |

**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<br>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<br>Dealing with historic users proves a constant issue for ISSs that undertake a transition to compliant status. Three months is not a long lead time for rebuilding architecture of a site or app, assigning development and engineering work. A gradual transition maybe required over a longer period but PRIVO recommends it is a staged process. |
| **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**

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**

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**

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**

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** |
| No<br>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** |
| No<br>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** |
| No |
| **14. Online tools** |
| No<br>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** |
| No<br>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<br>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<br>If YES, then please provide details (including links). |
| **2. Age-appropriate application** |
| No<br>If YES, then please provide details (including links). |
| **3. Transparency** |
| No<br>If YES, then please provide details (including links). |
| **4. Detrimental use of data** |
| No<br>If YES, then please provide details (including links). |
| **5. Policies and community standards** |
| No<br>If YES, then please provide details (including links). |
| **6. Default settings** |
| No<br>If YES, then please provide details (including links). |
| **7. Data minimisation** |
| YES/NO.<br>If YES, then please provide details (including links). |
| **8. Data sharing** |
| No<br>If YES, then please provide details (including links). |
| **9. Geolocation** |
| No<br>If YES, then please provide details (including links). |
| **10. Parental controls** |
| No<br>If YES, then please provide details (including links). |
| **11. Profiling** |
| No<br>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**

No

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

**14. Online tools**

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**

Yes

FTC Approved COPPA Safe Harbor Programs and GDPRkids™ Privacy Assured Program. www.privo.com and The Minor's Trust Framework - https://www.oixnet.org/registry/minors-trust-framework/

**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?

Yes

Behavioral advertising, remarketing, attribution and install tracking.

**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?

Yes

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/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

Audience definitions, advertising and marketing and device security in relation to children.

# Section 2: About you

**Are you:**

| | |
|---|---|
| A body representing the views or interests of children?<br>Please specify: | ☒ |

| | |
|---|---|
| A body representing the views or interests of parents?<br>Please specify: | ☒ |
| A child development expert?<br>Please specify: | □ |
| An Academic?<br>Please specify: | □ |
| An individual acting in another professional capacity?<br>Please specify: | □ |
| A provider of an ISS likely to be accessed by children?<br>Please specify: | □ |
| A trade association representing ISS providers?<br>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?<br>Please specify:<br>FTC approved COPPA Safe Harbor and GDPRkids Privacy Assured Program. About PRIVO: | ☒ |

**Thank you for responding to this consultation.**

**We value your input.**