Consultation on Age appropriate design: a code of practice for online services

Summary of responses

Introduction

On 15 April 2019 the ICO published the draft Age appropriate design code of practice for online services. Between 15 April and 31 May, the ICO ran a public consultation seeking stakeholder views. This document summarises the key themes emerging from the responses we received.

We received more than 450 written responses to the consultation, and we are grateful to those who took the time to comment. A copy of the responses we received from organisations is available here.

We carefully considered the views we received, which we used to inform the final version of the code. The ICO's responses to some of the key themes are included in this document.

A wide variety of both general and detailed issues were raised during the consultation. Whilst it is not possible to cover every point in detail, we have summarised the key responses to the questions asked. There are some overarching themes which cut across a number of the standards and we will refer to these throughout.

About the code (including services covered and glossary)

General points

Many felt that the structure and the layout of the code is clear and easy to navigate.

Most respondents, across all sectors, were supportive of the aims and ambition of the code in protecting the personal data of children. There were many, who commended the code and wished for its swift implementation in full; typically child development experts and bodies representing children's views and individuals, including parents. There were however some significant concerns, particularly from providers of

ISS and their trade associations, that more could be done to ensure the code is risk-based and proportionate.

There was also a general concern from some Information Society Services (ISS) and trade associations that the code could reach beyond the ICO's regulatory remit for data protection. Some suggested there was a risk that data protection and non-data protection issues are conflated in some elements on the code. It was also suggested that some aspects of the code cover activities already regulated by other legislation and rules. This could result in regulatory overlap, duplication or potential inconsistency and could overburden services which are already heavily regulated.

It was noted that the code may overlap with the Government's Online Harms White paper and that the two should be consistent. Where this was a particular concern for respondents, it is noted under the heading for the relevant standard.

Several respondents argued that the code should be principle and risk-based, with detailed technical information where required regarding implementation of its provisions. Some respondents felt that the current code needed a greater focus on this approach and is too vague in some areas and too prescriptive in others.

ICO response

We have amended the code to give providers of ISS more flexibility in how they wish to implement the standards of age appropriate design. The revised draft makes it clear that we will assess conformance to the code against the headline standards, and that the rest of the code is provided to give further explanation and guidance for those who need it. We have sought to stress the concept of conformity with the code and compliance with the law (GDPR).

We have also made amendments throughout to better explain and clarify the risk-based and proportionate approach, which takes account of the size and resources of the organisation concerned as well as the risks to children which might arise from the processing.

The final version of the code makes clearer that the ICO will also take a risk-based and proportionate approach to enforcement, taking into account the size and resources of the organisation, the risks to children inherent in the processing involved, and the efforts made to conform to the standards in the code during the transition period.

We are satisfied that the provisions of the code can be applied consistently with other legislation and codes of practice, and are flexible enough to take account of developments arising from the Online Harms White Paper. We are also satisfied that the provisions of the code fall within the ICO's remit and are sufficiently linked to the requirements of the GDPR and PECR.

'One size-fits-all'

Some respondents felt that the code took a 'one size-fits-all' approach, applying the same standards to various differing services. This was a factor in respondent's concerns that the code is not proportionate to the risks of the harm it is trying to protect from.

Some respondents suggested that particular sectors require an exemption, otherwise they will be disproportionately affected by the code. Suggestions for exemptions included public broadcasters and online publishers.

ICO response

The definition of services that fall within scope has been prescribed by Parliament in the DPA 2018. As the definition of ISS and the test of 'likely to be accessed by' is broad the standards need to be comprehensive enough to cover a wide range of different services.

We do not consider that s123 of the DPA 2018 allows the ICO to create exemptions from the code for specific sectors. However, as noted above, we have amended the code to allow services to take a flexible approach that is proportionate to the risks that arise from their processing of personal data. Following the consultation we have also included some specific content to address concerns about the freedom of the press and the rights of children to access information from the media online. Particular sectors are free to develop their own sector specific resources to sit alongside the code and the ICO will work with sector bodies on this where appropriate.

During the transition period for the code, the ICO also plans to help online services by procuring a package of practical support, including UX (user experience) design workshops.

Internet Society Services (ISS) and 'likely to be accessed by children'

Some respondents felt that the code needed to clarify what constitutes an ISS and provide some examples on what is/ is not covered. In particular, respondents raised questions about services used to access ISS and websites or apps, which may be interesting to children (such as online toy shops) but not necessarily aimed at them.

Many respondents felt there was ambiguity around the term 'likely to be accessed by children' and how this would apply to service in practice. For instance, some felt that the term as described in the code would apply to most if not all ISS, as a small number of children may access them. To assist in clarifying, respondents felt that it would be useful to have clear examples, or a clear threshold to assist them in determining if a service is 'likely to be accessed by children'.

For others, the scope of 'likely to be access by children' was simply too broad, which corresponds with comments about the code not being proportionate or risk-based. Instead, it was suggested that the scope of the code be narrowed to match other established principles such as the Committee for Advertising Practice's (CAP) Advertising Code. Others suggested that alternative wording should be used to narrow the scope, such as 'services directed at children', or 'services intended for children'.

Respondents noted that market research conflicted with the principle of data minimisation and that the code needs more clarity on its requirements for market research. Some felt that there was no legal basis for the code to recommend that ISS to conduct market research on its audiences.

ICO response

The scope of services covered by the code has been set by s123 of the DPA 2018. The ICO is bound to follow this approach set out in primary legislation. However, we have clarified our guidance about interpretation in light of consultation feedback. We have sought to provide greater clarity about the definition of an ISS, particularly for small business and those developing new online services. However, we note that the definition is taken from existing legislation that has wider application than data protection law. As such we would expect existing services (especially larger organisations with significant resources) to have already considered the question of whether they provide an ISS in order to comply with other legislative requirements.

We have sought to clarify the meaning of 'likely to be accessed by' in the context of the code. The DPA 2018 does not define 'likely' and there is no single definition of its meaning in UK law. Following the approach in Lord, R (on the application of) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin) (01 September 2003) we have therefore taken its meaning from the context in which the wording was introduced.

In doing so we have sought to recognise that Parliament used the wording 'likely to be accessed by', rather than narrower terms, to ensure that the application of the code did not exclude services that children were using in reality. This drew on the experience of other online child protection regimes internationally, that only focused on services designed for children and therefore left a gap in coverage and greater risk.

In light of this we consider that the possibility of this happening needs to be more probable than not for a service to be 'likely' to be accessed. We think this recognises the intention of Parliament to cover services that children use in reality, but does not extend the definition to cover all services that children could possibly access. We have amended the code to add these clarifications.

We have also included a flow chart in the code to assist in assessing whether the code applies. We have also amended the reference to market research to allow a more proportionate approach.

Jurisdiction and territorial scope

There were concerns from some respondents about the jurisdiction and territorial scope of the code. For example, that the code will impose requirements on UK companies that overseas competitors are not having

to comply with, putting UK companies at a disadvantage. Some respondents were concerned that non-compliant products could be available for download in the UK alongside compliant products.

ICO response

The ICO has no capacity to amend territorial scope in response to consultation comments as this is governed by the GDPR and the DPA 2018.

The GDPR territorial scope provisions ensure that not just EU-based companies comply with data protection law but also those offering goods and services from outside the EU to data subjects in the EU.

In any case we consider the standards in the code to reflect the existing requirements of the GDPR, such as the recitals related to protection of children's personal data, which apply EU-wide. The European Data Protection Board (EDPB) has also set out plans to develop guidance on children's privacy rights in its work programme for 2019 to 2020.

It is also relevant to highlight a number of international initiatives that address age appropriate design and protection of children's privacy, for example the Federal Trade Commission's settlement with YouTube and their current consultation on amending the COPPA rules. Other jurisdictions such as Australia and Ireland are preparing guidance. There are also initiatives from international organisations such as the UN Special Rapporteur and the OECD.

Costs and resources

Some respondents, particularly ISS and trade associations felt that the requirements of the code would be so costly that ISS might withdraw services from children or withdraw from the UK market entirely. Some standards evoked this response more than others, for example, geolocation, profiling and age appropriate application.

ICO response

We have amended the code to make it clearer that ISS providers can take a proportionate approach to conformance, taking into account the size and resources of the organisation as well as the risks to children inherent in the processing. The final version of the code also explains the proportionate and risk-based approach that the ICO will take to enforcing the code.

Whilst ISS providers are free to choose which markets they operate in, we believe that the code reflects shifting attitudes to the protection of children's data globally and that the code represents a significant opportunity to effectively enable the trust and confidence of children and parents and therefore confidence on the digital economy. The ICO wishes to see digital businesses operating in the UK sustainably adapt to the changes required by the code and we believe our approach will not lead to the risk some respondents identified.

There is a balance to be struck – we do not wish to see popular services withdrawn from the UK or from UK children, but the cost of these services cannot be the protection of children's privacy or maintaining the status quo where these issues are still too often an afterthought in the design process.

Respondents also raised this issue against other parts of the code and this response is intended to address these comments as well.

Timescales for implementation

Most respondents, across most standards, felt that an implementation period of three months was insufficient and instead believed a minimum of 12 months is required. Some argued that the measures detailed in the code would take several years to properly implement.

Where there were a large number of concerns about the transition period, we have detailed this within the summary of the standard.

ICO response

We have listened to concerns raised about the practical challenges of redesigning services to conform to the standards in the code. The final version of the code sets the transition period at 12 months which is the maximum period allowed by s123 of the DPA 2018. The ICO is unable to extend the transition period beyond this.

The ICO intends to further support ISS providers during the transition period by procuring a package of practical support including UX (user experience) design workshops.

The code also makes clear the factors that the ICO will take into account when considering any enforcement action, including the efforts made towards compliance during the transition period, as well as size and resources of the organisation and the risks to children inherent in the processing undertaken.

Enforcement

In general, respondents found this section was presented clearly.

Respondents noted the inconsistency in the definition of 'child' across various legislation, particularly as the age of a 'child' differs between the code and the 'digital age of consent' adopted by member states as required by the GDPR. As a result, some respondents believed the code shows a divergence from EU standards, making it difficult and confusing to adhere to.

In general, there was concern that the fines available to the ICO are disproportionate, especially to smaller organisations and should be reduced. It was suggested that the ICO should focus on engagement rather than fines and ensure that enforcement action is accompanied by 'lessons learned' communications and encouragement of best practice.

Respondents also wished for clarity around whether enforcement would be proactive or reactive and what legislative framework wound underpin the enforcement (ie the code is derived from the DPA 2018 but references the GDPR and PECR). Respondents also requested clarity on how organisations can demonstrate their compliance which may require a set of detailed criteria.

Finally, there was concern about the ICO's resources and ability to enforce the code, particularly internationally, which could be costly.

ICO response

The ICO acknowledges that there are enforcement challenges when working across borders but will continue to work with other Data Protection Authorities across Europe and globally in this respect.

The UNCRC defines children as 'every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier'. Neither the GDPR nor the DPA 2018 specifically define children but it is notable that Article 8 of the GDPR refers to consent being valid when 'the **child** is at least 16 years old' (13 in the UK). There is therefore no implication in the GDPR that children cease to be children when they reach the age at which they can provide consent to the processing of their own personal data. It is also clear from the debates when the Data Protection Bill passed through Parliament that their intention was for the code to apply to services likely to be accessed by under 18s.

During the Data Protection Bill, House of Lords Debate, 20 March 2018, c189Margot James, The Minister of State, Department for Culture, Media and Sport said:

> "It will also include requirements for websites and app makers on privacy for children under 18."

ICO response

Similarly the intention of Parliament in relation to the statutory underpinning of the code was made clear in Parliamentary debates.

During the Data Protection Bill, House of Lords Debate 11 December 2017, c1439, Lord Ashton of Hyde, The Parliamentary Under-Secretary of State for Digital, Culture, Media and Sport said

> "The new age-appropriate design code interlocks with the existing data protection enforcement mechanism found in the Bill and the GDPR. The data protection principles apply equally to children and are applied by data controllers on the basis of guidance provided by the commissioner. The GDPR makes clear that children merit specific protection with regard to their personal data as they may be less aware of the risks and consequences. The code will establish the standards required of data controllers to meet this obligation. The status of a statutory code means that any organisation that ignores it is taking a significant legal risk."

> "The code will carry the force of statutory guidance and set out the standards expected of data controllers to comply with the principles and obligations on data processors as set out by the GDPR and the Bill."

During the Data Protection Bill, House of Lords Debate, 20 March 2018, c189, Margot James, The Minister of State, Department for Culture, Media and Sport said

> "The code interlocks with the existing data protection enforcement mechanism found in the Bill and the GDPR. The Information Commissioner considers many factors in every regulatory decision, and non-compliance with that code will weigh particularly heavily on any organisation that is non-compliant with the GDPR. Organisations that wish to minimise their risk will apply the code."

However we have amended the code to make it clear that, in accordance with Part 6 of the DPA 2018, enforcement action can be taken when there is an underlying breach of the GDPR or PECR.

The final version of the code also explains the proportionate and risk-based approach that the ICO will take to enforcement action.

Standards of Age Appropriate Design

1. Best interests of the child

General

Respondents, especially academics, child development experts and child representative bodies, were strongly supportive of this standard. In particular, many felt that a child's best interests should be at the heart of design and that the code takes the evolving capacity of children into account. Some felt that if ISS adhere to the code, it will allow children to form their own opinions and make choices accordingly.

It was noted by some that the code should be clear that the 'best interests' should be from the child's point of view and not conflated with 'best customer service' or the views of their parents/ carers/ guardians. In addition, it was suggested that the code differentiate between short-term and long-term best interests, not allowing actions which are negative in the short-term to attain a long-term outcome which is in the child's best interest. Some respondents felt that the code should provide additional consideration for vulnerable children or those with additional needs.

Most respondents felt that the implementation of this standard may be difficult to achieve and require a fine balance. It was suggested that the code include a detailed balancing test to assist organisations.

Children's rights

Some respondents felt that the code focussed too heavily on the right to privacy under UN Convention on the Rights of the Child (UNCRC) and not the other rights under that convention. For example, it was suggested that the code's emphasis on restriction of content may impede a child's right to access information. Instead it was suggested that a delicate balance must be struck.

Implementation and transition

Others felt that the inclusion of this standard may stifle innovation and hinder design principles. In addition, this standard would require the inclusion of substantial changes which would affect all organisations, but may disproportionally affect smaller businesses. In order to make these changes, it was suggested by respondents that a longer transition period would be required, with some suggesting a minimum of 12 months.

ICO response

Data protection law is principle based and as such already requires ISS providers that process personal data to balance different interests and considerations and determine whether their processing is fair and proportionate. So whilst 'the best interests of the child' as an explicit consideration may be new, we believe it is consistent with existing good practice in the application of data protection legislation, including the relevant recitals related to protecting children's personal data.

We have added content to recognise children's right to access information from the media.

We acknowledge that additional considerations may require changes in design principles. It is our view that this will encourage more innovation, rather than stifle it. The ICO also intends to procure a package of support, including user experience (UX) workshops during the transition period.

2. Age appropriate application

Many groups representing children's views and child development experts were supportive of this standard in its current form. In particular, and as an example, one respondent appreciated the use of age brackets which acknowledge that older children's user habits can carry higher risk and are subject to decreasing levels of supervision over time, rather than treating all children the same.

There were also several concerns expressed about this standard. Some felt that it may be difficult to ascertain what is 'age appropriate' across multiple age groups and deliver a product accordingly. In particular, it was a concern that providing multiple services so there is an appropriate one for each age group would be difficult in practice, and in terms of cost, particularly for smaller organisations. Some argued that this may cause ISS to choose the youngest age group and design for them, resulting in poor design choices and poor user experiences.

Some common concerns raised for this standard overlap with those raised earlier, regarding the scope of the code and in particular the services covered. For example, concerns regarding what is meant by the term 'likely to be accessed by children' and failing to take a risk-based or proportionate approach. Also mentioned, was the potential confusion over the application of the UNCRC, which deems a child to be anyone under the age of 18, and the considerations of a child and the ability to consent in the GDPR, along with other regulations considering children. This could also make implementation difficult.

Respondents were concerned that the potential cost and difficulties of applying this standard could well result in ISS resorting to either apply the provisions of the code and treating all users as children, or to use age verification (AV). Another concern raised was that the requirement to include age appropriate defaults or verify a user's age will result in some ISS withdrawing from the market, or withdrawing access from children. In effect, it was suggested that this would remove child access to services, again in conflict with the child's UNCRC rights.

Age verification (AV)

Most of the concerns for this standard relate to the issue of AV. Many respondents had concerns about the use of AV. Respondents felt that more explanation could be provided to explain what 'robust' means in practice, with some suggesting that the code or the ICO suggest or provide a recommended method. This was a particular concern for some respondents, who felt there were no appropriate AV systems on the market. Others suggested that the code would stimulate innovation in the AV market and encourage the production of new methods.

It was suggested by some that use of AV results in the collection of more personal data than necessary, in contradiction to the principle of data minimisation. For some, the use of AV would result in additional information being stored and at risk of being compromised through a security breach or targeted by malicious actors.

Respondents expressed concern about the impact of AV on user journeys and experiences. There was specific concern that requiring age verification may prevent users from using a service, or frustrate them, resulting in a drop in users.

A significant number of respondents raised a concern about a perceived mandatory requirement to use AV, or that, as noted above, the approach taken by the code could result in ISS either applying the code to all users or 'age-gating' services entirely.

In contrast, some respondents praised the code, believing it strikes the right balance by not requiring age verification, but making it an alternative to applying the standards of age appropriate design by default.

Suggestions for AV

Some respondents suggested that the code limit any requirement to use AV to certain circumstances, for example if they have a large child user base, process sensitive data about children, or make impactful judgements using children's data. There was agreement that AV may be

an area where certification may be appropriate, perhaps under the remit of an AV regulator. It was suggested that AV may be best used in combination with other methods.

It was suggested that any requirement to age verify should not be implemented until the age verification provisions of the Digital Economy Act and the Online Harms White Paper have been considered and appropriately assessed.

ICO response

We have amended this section of the code to allow an approach which recognises the level of risk inherent in the processing.

Data protection legislation already requires ISS providers to assess the risks that arise from their data processing and to put in place measures that are proportionate to that risk. The final version of the code follows this approach by requiring ISS providers to establish the age of individual users with a level of certainty that is appropriate to the risks to children arising from the processing, or alternatively, to apply the standards in the code to all users. We believe this is a proportionate response which allows ISS providers some flexibility in how they approach this issue.

The code does not mandate age verification (though ISS providers who choose to rely upon consent as their lawful basis for processing should note that the GDPR does, and that following the provisions of this code may help them to meet this GDPR requirement in a proportionate way).

We do not see a contradiction between the code and the data minimisation principle of the GDPR. The data minimisation principle allows personal data to be collected if it is needed, as long as only the minimum amount of personal data needed is collected and it isn't used for other purposes.

The Government has now made a decision not to implement the age verification provisions of the Digital Economy Act.

Implementation

Given the complexity of re-designing services or implementing age verification, many felt that three months was not a long enough implementation period. Most suggested a minimum of 12 months, with some saying that any such implementation period should not begin until 'robust' AV methods are available in the market.

ICO response

We have recognised the work that may be needed during the transition period and have set this at 12 months. This is the maximum period allowed by s123 of the DPA 2018.

3. Transparency

Much of the response to this standard was positive, with many saying the section is clear and that it is positive that privacy information should be made understandable to all children.

However, respondents noted the difficulties in providing complex, often legalistic language in an understandable way, more so where children are concerned. There was concern that this may lead to the over-simplification of legal terms, undermining their accuracy. Some suggested that requiring different privacy information for specific age brackets may be unworkable, particularly because of the difficulty in assessing age. Others suggested that having to provide videos or pictures may affect the performance of apps, impacting on user experience.

Some respondents felt that the code conflates data protection issues with non-data protection issues by also referring to terms and conditions. It was suggested that this risks imposing concepts on children that they are unable to understand and that this may create a culture of fear. It was also suggested that it is problematic to direct children to rely on adults to provide guidance on using ISS as there is no guarantee that the adult understands.

ICO response

The ICO recognises the implementation challenges and intends to procure a package of support, including user experience (UX) workshops during the transition period to assist with this. We have also amended the code to allow for a more flexible and risk-based approach in deciding when different versions of information are appropriate.

We are satisfied that the provisions of the code are sufficiently linked to requirements of the GDPR and PECR and do not go beyond our data protection remit.

We do not see directing children to speak to trusted adults as problematic, given that it is only one of a number of measures designed to help protect the use of children's personal data, all of which are the responsibility of the ISS. We see it as part of the answer to the challenge of protecting children's personal data online, not a complete solution.

Implementation

Due to the time taken to re-design apps, roll out new privacy information and conduct user testing, many respondents felt a minimum of 12 months would be required.

ICO response

The final version of the code sets the transition period at 12 months. This is the maximum period allowed by s123 of the DPA 2018.

4. Detrimental use of data

Respondents felt that this section should be more detailed and provide examples of detrimental uses of data. In particular, some felt that the definition of 'detrimental' is too vague and risks conflicting with existing industry standards and the Online Harms White Paper. Others felt that the definition of 'sticky features' could be expanded upon.

The point was made that the code restricts activities in a precautionary manner where there is no evidence that the activity causes harm. It was suggested that this may dis-incentivise ISS from using data in legal ways. It was also suggested that it is difficult for an ISS to ascertain the impact on health and development, so a clear list of what is deemed most harmful is required.

Many were generally supportive of this measure, endorsing the references to the child's health and well-being.

ICO response

The ICO is not an expert on what is and isn't detrimental to children's health and well-being. For this reason we have drafted this section of the code to cross-reference expert advice, and to allow future developments in this area to be taken into account. We believe that our approach is consistent with Online Harms White Paper and that a precautionary approach is justified when there is official advice to take such an approach.

5. Policies and community standards

Some respondents welcomed this standard with some believing that ISS need to go further to moderate and enforce their terms and conditions to protect children. Some respondents suggested that the code could include example terms and conditions which should be used.

It was noted that the code may result in the enforcement of a provider's policies and procedures that were previously not enforceable. This may result in ISS reducing standards to avoid possible enforcement action. Respondents thought that a clearer explanation of how the ICO would monitor this standard would be helpful, including what the ICO would do to stop ISS from just adhering to a minimum threshold.

Another concern raised was that smaller organisations may not have the resources to moderate user-generated content to the required standards, resulting in a removal of the service from the UK market.

ICO response

This standard addresses the fairness issues that arise if an ISS provider collects personal data on the understanding that the service will operate in a certain way, and then does not keep to its own promises in this respect. It is not meant to define what terms and conditions a service must offer. It should work in conjunction with the other standards in the code, some of which do address more directly what can and can't be done with children's personal data.

6. Default settings

Most respondents felt that this section was clear, but could benefit from more examples, eg of what are and are not compelling reasons for applying different default settings, and what is meant by ‘high privacy’. In addition, it was suggested that the code could be clearer about what additional measures are required when a child attempts to change a privacy setting. Many respondents were generally positive about this standard with support from activists who believed this would change the dynamic of the internet and experience for children.

There were concerns, predominantly from ISS and trade associations about the impact of default settings on targeted advertising, personalisation of services and data sharing. Many felt this would result in a loss of advertising revenue and potentially mean free products must become paid-for products to continue to exist. Some felt there would be no benefit to treating all users as children, particularly adults who had already chosen their desired privacy settings. There were also suggestions that ISS might ‘age-gate’ their services to avoid having to implement high privacy default settings by default and potentially losing revenue.

Concerns were also raised about the practicalities of ‘switching on’ these new defaults and the effect of this on user experience and resources. For example, the user experience could be diminished by not allowing personalisation by default, or in some contexts, even defeat the point of the service (eg social networks). Others raised issues about parental involvement - specifically the risk of contravening the Children’s Online Privacy Protection Act (COPPA) in the USA, by allowing children to change defaults without parental consent and the risk of turning on parental consent tools without providing the child with choice.

ICO response

We believe this standard is fundamental to changing the way in which children's personal data is protected online. However we have made some amendments to the code to clarify when a privacy setting is not appropriate (eg because the core service can't be provided without the personal data being processed).

The consultation responses about the impact on advertising revenue indicated a general lack of awareness of the requirements of the GDPR and PECR which, regardless of the provisions of the code, mean that behavioural advertising requires prior consent from data subjects. We believe that 'off by default' is entirely consistent with the GDPR/ PECR consent requirements.

We believe that the code will not prevent services from complying with COPPA requirements. Whilst the code does not in itself prevent default settings from being changed, neither does it prevent parental consent to processing being sought before defaults are changed, if COPPA requires this.

7. Data minimisation

Many respondents felt data minimisation should be the standard, particularly for children. Some respondents suggested that children should be encouraged to use nicknames and pseudonyms when using online services, although this may contradict the policies of some ISS.

Whilst many respondents felt that this section was clear, aided by the use of examples, others felt that the particular examples used were not sufficient. Some ISS felt that allowing children to select what aspects of the processing to activate could be expensive and confusing to them, potentially resulting in poor service delivery if some data was missing.

Many respondents related their concerns about the use of age verification with how it may contradict the principle of data minimisation, particularly where they may now have to obtain more personal data than they currently do to verify a user's age. It was suggested by some that the ICO should carry out further research into how these two can be balanced.

As with many standards, concerns were raised about the resource implications of making such changes.

Other suggestions for further ICO guidance or policy development included:

- more detailed information on how much personal data can be collected from children;
- actively and knowingly engaged;
- deletion of data; and
- how to display opt-in and opt-out options.

ICO response

We do not accept that there is an inherent conflict between data minimisation and the collection of data to ascertain the age of a user.

The principle of data minimisation requires an organisation to collect only the minimum information required to achieve its purpose. An organisation should be able to process personal data in accordance with the data minimisation principle as long as it doesn't collect any more data than it really needs to achieve a level of certainty about the age of its users that is appropriate to the risks arising from its processing, and doesn't 're-purpose' the information it collects.

8. Data sharing

Many respondents were happy that the code included this standard, with particular reference to the child's best interests. These tended to be those bodies representing children. Some suggested that the code could go further, requiring any sharing of child personal data to be anonymised and prohibiting sharing of child data by third parties, unless for child protection purposes. Others requested further detail, particularly around what constitutes a compelling reason to permit data sharing.

However, some felt that the code needed to take a more risk-based approach and not disproportionately restrict the sharing of data. Some believed that to restrict sharing in this way was contradictory to the requirements of the GDPR, which allows this activity without requiring strict safeguards. It was suggested that some data sharing is positive and necessary for a service and this standard may result in an all or nothing approach being taken. Some felt this standard was one where the code sets standards that do not relate to data protection.

ICO response

We are satisfied that this standard is consistent with and sufficiently linked to underlying GDPR fairness requirements, and that it is flexible enough to allow data sharing in circumstances in which it is justified.

9. Geolocation

There were many positive comments about the inclusion of this standard, particularly that geolocation should be off by default. Some wished for the standard to go further, for example, by preventing children from being able to enable this at all.

Some felt that the code has interpreted geolocation as a completely negative feature, not taking into account potential safety benefits, particularly for children's parents. In addition, some geolocation is required to identify eligibility for use of a service, or for some connected devices to function properly, which some felt the code did not take into account.

ICO response

We have added content to recognise that for services where the core service cannot be provided without processing geolocation data (eg some mapping services) it will not be appropriate to offer a privacy setting which is off by default.

We do not think that a general position preventing children from enabling location services altogether is warranted. We consider that the existing drafting is flexible enough to allow 'positive' uses of location data where these can be properly demonstrated as justified, taking into account the best interests of the child.

10. Parental controls

Many respondents were pleased that the code recognised the role of parents and a child's right to privacy, in line with the UNCRC and without removing ISS responsibility. Some felt the code struck a good balance between these two often conflicting areas, whilst others suggested using a counter-signing process to get both the parent and child to agree to any parental involvement (parental co-consent).

The use of age ranges was seen as a benefit to some, who believed this would lead to different levels of control for different ages. In particular, they noted the possibility of children withdrawing from services if they felt they were constantly monitored. Others however felt the code should not require different controls for different groups, instead allowing one set of controls where these are suitable for all age groups.

It was noted by some that parental controls only work where parents/carers are willing and able to assist children. Some felt that the code needs to better consider families who may not be in the position to support children.

Some ISS and trade associations raised concerns about the practicalities of parental controls. In particular, it was suggested that it would be difficult to communicate complex information about parental controls to children, particularly those who cannot read. Others have suggested that this may be impossible for accessibility software, or in apps where audio-visual features may be unworkable. It was noted that if users are aware of monitoring, they will also be aware if their attempts to evade such monitoring are successful.

Some expressed concern that parental controls are currently some of the only safeguards in place and that extensive testing should be completed before any new requirements are introduced. Some argued that it is the parent's decision if their child knows they are being monitored and that the code oversteps data protection law in this regard. For some, this standard should not replace a conversation between parents and children and instead, the code should encourage engagement with children.

ICO response

We recognise that there is a fine balance for ISS to achieve in this area. The code does not require the inclusion or implementation of parental controls by ISS. Instead, it provides guidance for those who offer these controls about how to inform children and support conversation between children and their parents/ carers about this subject.

11. Profiling

Some respondents were positive about this standard, with some suggesting that the code could go further, for example, by preventing profiling of children for behaviourally targeted advertising, prohibiting profiling unless it is essential, or preventing it in any circumstances.

Others felt there should be a clearer distinction between interest and contextual-based advertising, where the latter uses anonymised data.

Some respondents noted the benefits of profiling, for example, in identifying younger users and blocking inappropriate content, generating insurance premiums, educational and care settings and improving game experiences. Instead, some suggested that the code take a less restrictive approach, bearing in mind that the GDPR does not prohibit this activity, but provides safeguards.

On this theme, some respondents felt that if the code did not take a less restrictive approach user experiences would be degraded and children would suffer from consent fatigue. In addition, respondents explained that revenue streams are often reliant on targeted or personalised advertising, without which many services would no longer be able to operate.

Some felt the code would be particularly difficult to apply on shared/ family devices where tailored and personalised user accounts are necessary.

There were suggestions that profiling is necessary for the types of tailoring required elsewhere in the code. Some respondents felt that ISS would be more likely to withdraw services from children than navigate between providing tailored content where required and the provisions about profiling.

ICO response

We believe that the code takes a proportionate approach to profiling, not prohibiting it, but ensuring that appropriate measures to prevent harm are put in place, if it does happen. It provides sufficient flexibility for profiling to be 'on by default' if this can be properly demonstrated as justified, taking into account the best interests of the child.

The consultation responses about the impact on advertising revenue indicated a general lack of awareness of the requirements of the GDPR and PECR which, regardless of the provisions of the code, mean that behavioural advertising requires prior consent from data subjects. We believe that 'off by default' for this type of profiling is entirely consistent with the GDPR/PECR consent requirements.

We have added content to address profiling that might be necessary to meet the requirements of the code.

12. Nudge techniques

Many respondents were supportive of the code's stance for this standard and believed the requirements were clearly set out and demonstrated with examples. Some felt that further explanation of what constitutes a 'nudge technique', 'sludge technique' or a 'sticky game feature' is necessary. Examples of real life nudges and their damage, for example in games, were also requested from respondents.

The inclusion of 'likes' as a persuasive feature was criticised by some who believe that giving and receiving likes were important for freedom of expression and the development of confidence for children. It was suggested that the code take a more evidence-based approach which looked at actual harm when determining what techniques should be restricted or prohibited.

Some respondents felt that the code should only introduce restrictions where the nudge techniques relate to the collection or personal data or have privacy implications. Some felt that by looking at wellbeing, rather than data protection issues, the code was going beyond the provisions of the DPA. There was general concern from some respondents that the provisions of the code would be detrimental to business as it would require a radical redesign and prevent encouraging users to complete abandoned transactions, reducing revenues.

ICO response

We have amended the final version of the code to make it clearer that the code is concerned with nudges related to the use of personal data. We have also moved the content on 'strategies used to extend user engagement' to the section on detrimental use of data, again clarifying that we are concerned with such strategies that rely upon the use of personal data.

13. Connected toys and devices

Some respondents welcomed these provisions and believed they were provided clearly within the code. It was suggested that further details could be provided on what constitutes a connected device. Others suggested this section would benefit from being split into different categories, as follows:

- connected toys;
- wearables (including smart home devices and hubs); and
- services designed solely for educational use.

There were concerns amongst ISS and trade associations about the practicalities of updating existing connected toys and devices. In particular, it was suggested that this may result in wastage and instead, users could be informed that their existing devices are non-compliant. It was suggested that the code reference the Code of Practice produced by the Department for Culture, Media and Digital for the Internet of Things consumer security.

ICO response

We have added content to this section to address concerns about transitional arrangements, manufacturing cycles and existing stock.

14. Online tools

Respondents were happy about the inclusion of this standard and many found this section clear. Some felt that it should also require ISS to prioritise children's requests to exercise their rights and, or their reported issues, and to contact the child to inform them about the outcome. Others have suggested additional tools which should be required, including tools to show a user who has accessed/viewed their data, a tool which shows what has been inferred/derived from their data, etc.

There were concerns from ISS that implementing this standard would be a significant engineering challenge, with one suggesting that it could take years to implement. Others requested clarity on when a parent would be able to exercise their child's rights on their behalf. Further detail was also requested where distressing content is included, particularly about the speed with which the ISS should remove the content. Some suggested that whilst the concern is investigated, the ISS should be obliged to remove the content where it relates to a child immediately, rather than waiting for the outcome.

ICO response

The ICO acknowledges the challenges that this standard raises and intends to further support ISS providers during the transition period by procuring a package of practical support including UX (user experience) design workshops.

15. Data Protection Impact Assessments (DPIAs)

Respondents were generally supportive of this standard and thought it was clearly explained. Many believed it was important to set out data protection considerations about the intended use of children's data and evidence decisions, not only for compliance, but for transparency purposes too. It was suggested that the code could require a DPIA to include clarity in consent framework and children's ability to understand and activate their rights. In addition, the DPIA should address vulnerable children or those with additional needs who may lack capacity to consent to processing.

Some felt that DPIAs may be costly, particularly if they require legal input, and may be a barrier for smaller organisations. Some suggested that the code 'moves the goal posts' for DPIAs from data protection issues to issues like self-esteem and peer-pressure. For some respondents, the requirements of the 'child-friendly' DPIAs are onerous, particularly having to consult with children and parents. In addition, it was suggested that re-doing existing DPIAs will be poorly received by industry and take up considerable resources.

ICO response

We have made it clearer that the risks to be considered in a DPIA are those which arise from the processing of a child's personal data. We have also allowed a risk-based and proportionate approach to consultation with parents and children.

The requirement to conduct DPIAs, including for existing services is found in the provisions of the GDPR. The final version of the code provides risk-based and proportionate guidance to ISS about how best to complete the DPIAs for services likely to be accessed by children.

16. Governance and accountability

Generally, respondents felt this section was clear. Some respondents supported these provisions, for some of the same reasons as set out above on the section on DPIAs.

Respondents felt that the code should ensure it does not conflict with the Online Harms White Paper, which was a concern throughout the code. In addition, it was suggested that the ICO and Government could provide more guidance and best practice advice on how these obligations interact with each. An example of an area where this may be needed was about'compelling reasons' for data gathering in relation to safeguarding.

There were some concerns about the code making clear how it applies to different parts of the supply chain and which companies control what data.

ICO response

We believe that the code is consistent with the aims of the Online Harms White Paper and flexible enough to take account of any new developments that result from it.

We will work with other regulators as appropriate, which can include Memorandums of Understanding (MoUs) and other joined up ways of working, as illustrated by the MoUs and co-operation that the ICO has with the FCA, CMA, Ofcom and other regulators.

Annex A (now Annex B)

Most respondents felt this was sufficiently clear. Some arguments were put forward around adjusting the age ranges suggested in this annex, particularly about aligning these with other codes of practice.

Annex B (now Annex C)

Generally respondents felt this section was clear. Some felt that some of the language was more legalistic and complicated than in the other annexes and could therefore be refined.

ICO response

This annex contains more legalistic and complicated language due to the nature of its subject matter. The ICO has to communicate guidance on lawful bases in a concise and understandable way, but must also be careful to not change the meaning of important concepts.

We are satisfied that we have communicated the information in Annex C (formerly Annex B) in the most precise and accessible way possible.

Annex C (now Annex D)

Most respondents felt this annex was clear. Suggestions for improvement included redesigning the DPIA template to give the prompts in section 2 their own boxes or introducing an online interactive version of the DPIA.

General comments

Some respondents, particularly amongst ISS and trade associations felt a longer consultation period was needed and that six weeks was not sufficient. In addition, some suggested that the ICO should conduct a formal economic impact assessment before the code is finalised.

Some felt that the code itself does not recognise that not all online services are harmful, or have harmful impacts on children. Whilst some respondents felt that introduction of the code would stifle innovation, others felt that it provides incentives for economic growth, innovation and developing ethical bases for services.

ICO response

We have consulted on the code throughout its development in the following ways:

- an initial, open, call for evidence;
- consultation with children and parents via a specialist research provider;
- an open consultation on the draft code;
- face-to-face meetings with key stakeholders during and beyond the consultation period; and
- consultation with Government via the DCMS.

This process set out above has enabled the ICO to understand the practical implications of the code at different stages of the policy development, including how the code will effect digital businesses.

The changes made to the code during this process reflect the ICO's approach of balancing the ambition for the code to provide effective protections for children's personal data online, building sustainable trust and confidence in the UK digital economy and ensuring that code is fair, practical and proportionate for business.

DCMS has confirmed that an economic impact assessment is not required as the code explain existing legislative requirements rather than introducing new ones.

Recommendations for research

Many respondents suggested areas which the ICO could produce further guidance, or conduct further research. Suggestions for further research/actions included:

- Economic impact assessments of the code.
- An assessment, once the code is introduced, on the impact of the code on children and their privacy.
- Robust age verification systems and their relationship with data minimisation.
- Engagement and promotional work around the code for children and young people, including making child friendly versions of the code.
- More research into the views and roles of parents in achieving the code's aims.
- Engagement/workshops with ISS to support practical application of code.

ICO response

The ICO currently runs a number of programmes intended to help organisations research and innovate around data protection and privacy issues. For example, the ICO grants programme and regulatory sandbox.

In addition, the ICO also intends to procure a package of support, including user experience (UX) workshops during the transition period.

Next steps

We submitted the final version of the code to the Secretary of State on 22 November 2019.

The Secretary of State must then lay it before Parliament as soon as reasonably practicable.

The code will remain before Parliament for 40 sitting days. Unless Parliament resolves not to approve the code within that 40 days, the Commissioner will then issue the code and it will come into force 21 days after that.