DIGITAL
POLICY ALLIANCE
informing policy for a competitive, inclusive, networked society

**Age Verification & Internet Safety
Working Group
Consultation Response**

September 2018

Age Appropriate Design Code

The Digital Policy Alliance thanks the Commissioner for providing us with the opportunity to comment on your call for evidence regarding the development of an Age-Appropriate Design Code.

In many ways, the proposed code will need to pre-suppose that the provider knows the age of its intended audience before applying appropriate design to the user interface. However, behind the scenes of how information society services work, we think that there are some very important principles of age check practices and challenges that we would like to draw your attention to.

In developing our response, we would first of all draw your attention to the detailed and considered response by the 5 Rights Foundation to this call for evidence. We would fully support that response and don't intend to repeat in our response below, but do want to elaborate on some of the points that they make.

The Code must offer a high bar of data privacy by default.

It is our view that the age check practices of information service providers (including joining age, community rules and any age appropriate commitments made in terms and conditions and privacy notices), should be subject to routine, random, 3rd party monitoring and review, with non-conformities identified to the service provider and actions required to rectify the issues.

The routine failure by a provider to adhere to its own published rules on these matters, such as a failure to maintain certification, should be considered to be evidence of a breach of the Code. We would not press for certification to be a requirement for the Code, moreover that certification could be mentioned as a method of demonstrating and maintaining evidence of conformity. The principles of 'earned recognition' in the Regulators Code should be applied to the intelligence gathering and choices on the deployment of enforcement resources by the Commissioner - in other words, a certified information service provider for age appropriate design ought to attract less attention of regulators than a non-certified provider.

The certification scheme(s) - which could be an extension or subset of ISO 27000 series or PAS 1296:2018 - would include specific requirements relating to privacy by design and reflecting the requirements of the eventual Code. The PAS 1296:2018 is a new Code of Practice for Online Age Checks published by the British Standards Institute earlier this year.

It follows that industry self-regulation through certification should be the first, expected approach to be taken - but to be effective, this must be supplemented by a proportionate and escalating enforcement regime by the Commissioner with the appropriate skills and resources to effect behaviour change in the industry. This also needs to include for international cooperation and standards development.

A particular challenge with this may come from the inter-operability of the 'safe harbor' program operated by the Federal Trade Commission under the Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. 6501–6505. Like it or not, many information society services emanate from the US or are principally based in the US. They regard compliance with COPPA as being the standard to which they work to - be that the standards set up by iKeepSafe, iVeriFly or any of the other 'safe harbor' authorised providers.

COPPA is now 20 years old and is somewhat out-of-step with the developments of information society services; its sets a low bar for securing age appropriate controls on websites. The major challenge for the Commissioner will be getting international website providers, wedded to and comfortable with the limited requirements of COPPA, to embrace and adopt a UK-based Age-Appropriate Design Code - backed by enforcement penalty.

Eventually, of course, COPPA and similar provisions may catch up and the UK's Design Code could be a catalyst for that happening, together with other moves to develop age appropriate controls.

Creating an expectation of challenge

Where young customers approach an 'age gateway' then information society providers should generate an expectation of challenge in the manner, layout & presentation of their service - both in the user journey and in their ethos, ethics and marketing of their services. The expectation of challenge starts before the young person even visits the website.

As an example, age appropriate design, needs to include how websites are marketed - if websites are intended for teenagers (the 12+ range for instance), marketing and advertising them in junior schools should be considered contrary to the principles of the Age Appropriate Design Code - in other words, the Code needs to be more than just about the design of the site, it is about the consideration of the target audience and the ethos and ethics of marketing the site.

The expectation of challenge continues throughout the journey of the user. As children approach an age gateway, they must be expecting it and be anticipating that their attempts to get through the gateway unchecked will fail. It follows then that the age gateway must be meaningful.

The self-selection of a date-of-birth must not 'encourage' pretending to be older. This can have very serious consequences that would not necessarily be on the mind of the child when creating an account with an information society provider. As an example, if a website is suitable for only those aged 13 or over, a weak age gateway could ask the user to enter their date of birth, but only provide them with an option to select a date up to 2005, for instance. This is how the age gateway on Facebook, for instance currently works. This is wholly inadequate and poor design. It encourages the user, even if they wanted to put their correct date of birth, simply to use the latest available date. What that means is, on the date of signing up to the account, the age gateway will show that they are 13, even when they are in fact only 11 because they were unable to select 2007 as a year of birth.

Fast-forward 4 years, the child will likely never have changed their incorrect date-of-birth, either having never been prompted to do so. They are now interacting with people through social media, their online profile showing them as being 17 when, in fact, they are only 15. This could continue through life, but more concerningly, could it be said that a potential groomer or sexual predator could 'claim' that they had reasonable grounds to believe that the user was over 16, because that was the age shown on their profile - whereas they were in fact under 16?

Equally weak age gateways include the ability to enter a date of birth (the first entry being correct), access to the site being rejected on the grounds that the user does not meet the age policy/requirement for the site, but that same user then being able to just go back, change their date of birth and still get on. Age appropriate design should exclude the possibility for someone to simply side-step the requirements in this way. If site operators are going to use 'cookies' to help their sites processes to work, they should, at least, be able to make them do something positive like track where someone entered 11/08/2008 to get set up on a 13+ website, and when declined, simply entered 11/08/2005 instead.

Given GDPR mandates data minimisation, there is an obligation for ISS providers to only ask for an amount of personal information proportionate to the service they wish to offer. In the context of age verification, it is generally if someone is above or below a certain age to be eligible for a service, rather than their exact date of birth. Hence organisations and regulators are now able to encourage data minimised solutions which are asking for just under 13 or over 18 rather than requesting a person's exact date of birth.

Privacy Notices

The ICO recommends a layered approach to privacy notices, with clear content and presentation. We would support the current approach, rather than a focus on maximum word count given that greater transparency is also required; which generally means explaining something complex in a longer but simpler way.

Broad audience versus child audience

We would encourage the ICO to consider carefully the difference between services designed for a general audience versus services targetted specifically at children. This is a useful distinction made by COPPA, with clear guidance laid out by the FTC as to what constitutes a 'child directed service'. Indeed there may be generalist services which are designed specifically with privacy in mind, for instance password managers, which (although they may require parental consent) purposefully set up privacy protection in a way that they do not know which are adult and which are child users.

Clearly there are educational and online safety products and services which are designed for a general audience for whom working with narrow age bands would not be feasible. This would in particular discourage SME providers from delivering those services to under 18s where considerable resource and investment is required to support the design, build and maintenance of multiple versions of the same product for different age brackets. Care should equally be given as to the number of age brackets required for exactly this reason. Otherwise, this could lead to more consolidation and market dominance by the larger players. On the other hand, we concur there is definitely a need to review the approach of ISS services which are aimed at children.

Holding Information Society Services to Account

Many information society services offering clearly child directed services have publicly stated commitments to 'age-appropriate' design, controls and policies. These are often somewhat loose and without methods to hold them to account, often meaningless. So we would like to see Childhood Impact Assessments as standard for all existing services and products that target children, and new services and products prior to launch. This is effectively getting website operators to 'nail their colours to the mast'. Rather like Corporate Social Responsibility commitments, these are only of any real value if they are acted upon, reviewed and independently assessed to secure the commitments made. The "move fast and break things" and "fail furiously" culture of the technology industry does not hold the best interests of the child as their primary consideration. Introducing child impact assessments before services and products are rolled out would circumvent some of the most obvious data risks. The Commissioner might consider using the Responsible Innovation Framework as defined by the Engineering and Physical Sciences Research Council.

Ultimately, whilst we are supportive for child targeted services to advocate self-regulatory approaches such as Child Impact Assessments, Corporate Social Responsibility, Certification, Monitoring and Audit, to be effective the self-regulatory approach must be backed up with meaningful, resourced and active enforcement. Those responsible businesses that do take a considered and careful approach need to be assured that their competitors (often simply competing on traffic volumes) are not handed competitive advantage by lax or non-existent enforcement. They also need to see being responsible rewarded with recognition, both officially and through the internet eco-system. As an example, search engines may include 'bounce rates' in their algorithms determining search position. A responsible age-appropriate design page with suitable age gateways will, inevitably, have a higher 'bounce rate' than a more open irresponsible site - yet the open site with the lower 'bounce rate' could be rewarded with higher search position. The broader internet eco-system has to develop ways to encourage responsibility, not irresponsibility.

Similarly, the provisions of the Regulators' Code need to be applied to the work of the Commissioner - notably 'earned recognition' of being able to demonstrate compliance through independent 3rd party auditing, monitoring and certification. The Commissioner needs to take that into account when making intelligence-led tasking decisions for enforcement activity. This also provides the Commissioner with a justification to accelerate the regulatory ladder of intervention (i.e. take action, quicker, more severely and at a higher level) as she will be able to point out that providers have a means and opportunity to avail themselves of self-regulatory schemes that are out there - failure to do so (and the requisite evidence of non-conformance) would tend to indicate that a more severe, higher penalty be imposed - thus, of itself, encouraging others to avail themselves of the self-regulatory schemes.

This only works though if the providers can be held to account and the government commits the resources to the Commissioner to enable her to take appropriate action. Unless there is a meaningful likelihood of enforcement, then the providers are not incentivised to implement the Code in ways that are robust and effective. The ICO needs sufficient expertise and resources, and given the huge wealth of some ISS, the backing from treasury to fund enforcement.

We hope that our submission will be of assistance.

Freedom of Information Act - Please be advised that we do not consider anything in our response to be confidential and we would be content for it to be published by the Commissioner or made available in any response to a Freedom of Information request. We would ask the Commissioner if referring to our response in any report to kindly attribute them to us.