ICO's Children's Code Strategy 2024-25: 5Rights response

5Rights Foundation
Call for evidence response
October 2024

Background

In August, the UK's data regulator, the Information Commissioner's Office (ICO), published a call for evidence on its 2024-25 strategy for the Children's Code (the Age Appropriate Design Code or 'the Code').[1]

The Code, which was brought in by the 2018 Data Protection Act and has been enforceable since 2021, is the first of its kind in the world – setting out 15 standards that digital services likely to be accessed by children must follow. The Code has been replicated and had impact globally, leading to a number of key design changes at major tech companies in the name of children's privacy and safety.[2]

As part of the call for evidence, the ICO sought views on the Code in the round – including its impact, enforcement and if changes were needed. Below we have published our response to this part, highlighting where we believe the ICO must go further and robustly enforce the Code.

Response

What changes would you like to see the ICO's Children's Code strategy deliver for children that use social media and video-sharing platforms (VSPs) in the UK?

5Rights is proud to have helped make the case for the creation of the Age Appropriate Design Code (the Children's Code, or 'Code') in the UK and continues to work with industry and the ICO to ensure services design data practices that put the best interests of children above all other considerations, in line with its foundational aims.[3]

We welcome the ICO's renewed focus on the Age Appropriate Design Code. In the three years since the Code came into force, its impact has continued to reverberate globally.[4] As the ICO highlights, the Code has led to a number of significant design changes in the

---

[1] Information Commissioner's Office (2024) *Children's code strategy call for evidence*

[2] Wood, S. (2024) *Impact of regulation on children's digital lives*, Digital Futures for Children Centre, 5Rights Foundation and London School of Economics and Political Science

[3] Baroness Kidron, 11 December 2017, Data Protection Bill [HL], Vol. 787, Cols. 1426-1428

[4] See: 5Rights Foundation (2024) *Celebrating 3 years of the Age Appropriate Design Code*

name of children's privacy and safety[5] and continues to inspire countries and states around the world to adopt similar standards. Most recently, the Australian Government announced that it would be bringing forward its own Children's Privacy Code based on the standards of the UK Code.[6]

However, it is unacceptable that compliance with the Code has been inconsistent and selective across all services likely to be accessed by children. This piecemeal approach has been allowed by the ICO because it has taken very little action to enforce the Code and, when it has acted, it has not done enough to communicate its decisions to ensure others in the sector can understand what is expected – raising the bar across the whole industry.

Large-scale and non-compliant misuse of children's data places regulated services at odds with the Age Appropriate Design Code. The ICO's duty is to robustly enforce compliance.

Below we make three recommendations that the Code's strategy must address:

1. The strategy must focus on services with high-risk data processing

The ICO has selected social media and video-sharing platforms (VSPs) as its focus for the 2024-25 strategy, owing to the vast numbers of children that can be found on these services. If the stated aim is to safeguard against the misuse of children's data, the size of a service does not always mean that it is the riskiest – there are countless examples of different categories of service, as well as smaller services, creating catastrophic risk to children.

For example, data processing in education technology (EdTech) products poses a very high risk to children given how it can impact a child's future prospects.[7] Online gaming services can be high risk if the data processing is used to encourage children to buy in-app items or currency, such as lootboxes.[8]

It was not part of the Code's intention to omit certain sectors or actors from compliance; rather that all digital services likely to be accessed by children must comply. We do not understand the basis on which the ICO believes it is appropriate to narrow the application of the regime from Parliament's intention.

All four of the ICO's priority areas within this strategy (default privacy and geolocation settings; profiling children for targeted advertisements; using children's information in recommender systems; using information of children under 13 years old), if properly enforced in children's best interests, are relevant beyond social media and VSPs. For

---

[5] See also: Wood, *Impact of regulation on children's digital lives*

[6] Office of the Australian Information Commissioner (2024) *Better privacy protections for children are coming*

[7] See: Mon-Williams, M., Elshehaly, M., and Sohal, K. (2022) *Connected data for connected services that reflect the complexities of childhood* in Livingstone, S., and Pothong, K. (Eds.) (2022) *Education Data Futures: Critical, Regulatory and Practical Reflections*, Digital Futures Commission, 5Rights Foundation

[8] Atabey, A., Pothong, K., & Livingstone, S. (2023) *When are commercial practices exploitative? Ensuring child rights prevail in a digital world*

example, the importance of default privacy settings is just as relevant to online gaming services as it is to social media, profiling for targeted advertisements is just as relevant to digital marketplaces as it is to VSPs, and preventing use of information of children under 13 is relevant across the entire digital environment including apps, search engines and messaging services.[9]

Recommendations: The ICO should make clear that all services likely to be accessed must be compliant and it should publish information about which services are subject to further inquiries or investigation, as well as enforcement decisions. Where it finds against one organisation, or a company makes changes to its service in response to further inquiries or investigations, the ICO should publish information about these changes so that all services likely to be accessed should meet the same bar.[10]

The ICO should also develop a framework for what constitutes high-risk processing using examples of how children really use the online world and make clear that all services with high risk strategies should meet the highest bar of compliance with the Age Appropriate Design Code.

2. The strategy must address how the Code and Ofcom's Children's Safety Code of Practice are distinct to avoid a diminution of standards and compliance

With the Online Safety Act's Children's Safety Code of Practice due to come into force next year, the ICO must provide guidance for how services in scope of both regulations can and must comply with each Code separately, to ensure there is no diminution of compliance with the Age Appropriate Design Code. There are measures in both codes which, although similar, have important distinctions.

Privacy/geolocation default settings

Default privacy settings, such as turning geolocation settings off by default each time a child user enters a service and reverting these settings to 'off' after each use, is a clear and distinct standard of the Age Appropriate Design Code.[11] This is an essential part of preserving children's privacy, while also keeping them safe online. While Ofcom's draft Children's Safety Code will also require geolocation to be off by default as safety measure,[12] there is no detail yet if this will include reverting settings every time a child user ends the session. For example, the ICO has not acted against Snap, whose *Snap Maps* function does not default off after a child has stopped using it. As in the previous

---

[9] See: 5Rights Foundation, Digital Futures Commission (2023) *Child Rights by Design* toolkit, which is aimed at developers and innovators of *all* services that children use or are impacted by, includes embedding privacy by design as a core aspect of product development

[10] The Information Commissioner's Office (2024*) What we learned from reprimands* should be formatted and adapted to produce a specific version for the Age Appropriate Design Code

[11] Information Commissioner's Office (2021) Age Appropriate Design Code, *Standard 10: Geolocation*

[12] Ofcom's draft Illegal Harms Code of Practice, which sets out measures for default settings applied to by children and is replicated in the Children's Safety Code of Practice, proposes Measure 7A on geolocation. Ofcom states in Vol. 4, 18.3(d) that "the ICO's Children's Code highlights the importance of children being aware that their location is being shared, through their requirements that geolocation sharing options be switched off by default and that child users are made aware if their location is being tracked"

section, we believe the ICO to be remiss in failing to deal with such a clear lack of compliance.

Recommender systems

Ofcom's Children's Safety Code also includes draft recommendations for how services must prevent recommender systems pushing harmful content to children. The Age Appropriate Design Code has similar standards but extends beyond content and requires services to factor how algorithms push children to expand their social networks (e.g. ranking comments and recommending connections to children) and how they extend use. Under the ICO's Code, services are required to think about how their commercial strategy can mitigate these risks.

For example, if a service's growth depends on a social connection strategy which recommends a 'friend' connection between two users just because they follow the same pop star, this would not constitute a sound basis for recommending that connection to a child because it means they are being recommended to a stranger with whom they have no previous relationship or connection.

In the work we do with children, they frequently report adult strangers making friend requests.[13] These forms of recommender systems, or recommending products, services and features and functionalities based on interests, clearly involve using children's data for profiling. Many of these recommendations are not in their best interest, and others are deliberately extending use and are therefore non-complaint with the Age Appropriate Design Code. As such, it is of concern that the ICO's proposed strategy is limited to recommender systems that relate to content only.

Recommendation: Noting that the previous Information Commissioner had already written that it is "unlikely that a commercial interest would ever trump the best interests of a child",[14] the ICO must be clear on what is in scope of its regulatory oversight powers and not simply fall into line with Ofcom's approach when it is a lower standard. This strategy could help deliver for children by ensuring that services are under no doubt as to their obligations for both Codes, which are clear and distinct.

3. **The strategy must address how children's data protection applies in generative AI systems**

The rapid growth and development of generative AI and the Government's intention to see it integrated into public services[15] will have major implications for children's data and privacy: from the immediate impact, such as the use of their data to create child sexual abuse material (CSAM), to the long term impact, such as the use of their data in AI EdTech products which purports to help teachers save time on administrative tasks.

---

[13] See: 5Rights Foundation (2021) *Pathways: How digital design puts children at risk*, p. 63

[14] See: Age Appropriate Design Code, *Standard 1: Best interests of the child* which states "It is unlikely that the commercial interests of an organisation will outweigh a child's right to privacy"

[15] Department for Science, Innovation and Technology & Department for Education (2024) *Teachers to get more trustworthy AI tech, helping them mark homework and save time*

Children are at the knife-edge of these new systems, yet they are entirely missing from the conversation about how we make it safe for them to use.

The ICO must ensure children are integrated and embedded at the heart of its strategy on AI. The ICO has recently produced guidance that appeared to suggest that AI scraping must observe GDPR,[16] and therefore the Age Appropriate Design Code.

Recommendation: The ICO must provide an explanation for how the Age Appropriate Design Code must be applied by AI companies, including in the design and deployment of Large Language Models (LLMs). If it is the ICO's view that the Code will not include these systems or that it is not sufficient, then it should identify the limits of its powers and report this publicly as well as to the Secretary of State for Science, Innovation and Technology.

To what extent do you support the action that the ICO is taking to ensure that social media and video-sharing platforms (VSPs) comply with data protection law and conform with the standards of the Children's Code?

It has always been 5Rights' ambition that companies would use their creativity to innovate in order to comply with the Code, rather than have the ICO force compliance retrospectively. However, three years into enforcement of the Code we regret that, despite egregious and continuous lack of compliance with the Code, the ICO has failed to take action in any meaningful way. This includes where 5Rights has provided evidence of misuse of children's data.[17]

We note that the ICO has not yet issued a single fine for breaches of the Age Appropriate Design Code and, where it has worked with companies to make (what have been rather minor) changes, they have taken no action for these decisions to become sector wide expectations of compliance.

We highlight below issues with the ICO's approach to enforcement.

1. Transparency

We welcomed the recent announcement that ICO has sent notice to 11 services for breaches of the Code,[18] but we disagree with the decision not to name them. Companies in breach being subject to heightened scrutiny is a matter of public interest and is, in itself, an act of enforcement.

Moreover, the failure to name them denudes the public of their right not to trust them and, as previously stated, does nothing at all to set a sector-wide bar. Finally, it is bad regulatory practice for a regulator to protect regulated services in such a way, and it

---

[16] See: Information Commissioner's Office (2024) *Generative AI first call for evidence: The lawful basis for web scraping to train generative AI models*

[17] 5Rights Foundation (2024) *5Rights challenges Meta's inaction on AI-generated CSAM*

[18] Information Commissioner's Office (2024) *Children's Code Strategy progress update*

lends weight to those who believe the poor form of the ICO is due to regulatory capture.

2.   Defence of the Age Appropriate Design Code in any proposed data reform bill

The Government has announced that it will be bringing forward legislation to reform data protection in the UK. It was notable that the ICO did not defend either UK GDPR or the Code against proposed changes by the previous government, which would have watered down protections for children. It is also notable that the ICO, in spite of its clear problems in enforcement, has not asked for greater powers to make the Age Appropriate Design Code directly enforceable.

3.   Age-appropriate design and data processing

We note that this strategy does not discuss age-appropriate design, despite this being a vital feature of how services complying with the Code can safeguard children. We would like to see greater enforcement action and auditing from the ICO which looks at how services are recognising that children have different capabilities and needs at different ages.[19]

4.   An independent review

In spite of repeated attempts to engage, inform and support, the ICO has failed to enforce the Code, articulate what obstacles it has to enforcement so that new powers could be granted, and, where changes have been made, they have been hidden from sight and/or not communicated as industry wide standards.

The new strategy further diminishes the Age Appropriate Design Code by focusing on a subsection of the tech sector rather that all services likely to be accessed by children, and on a subsection of the 15 standards rather than the interconnected standards of the regime. We recommend the Government set up an independent review of the ICO, to ensure transparency of and optimise its processes and functions for the effective enforcement of the Age Appropriate Design Code.

[19] Both the United Nations Convention on the Rights of the Child (1989) and its General comment no. 25 (2021) on children's rights in relation to the digital environment both require states to respect the" evolving capacities" of children

About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the lived experiences of young people.

5Rights is a registered charity. Charity number: 1178581.