ROB BONTA
Attorney General of California
ANYA M. BINSACCA, SBN 189613
Supervising Deputy Attorney General
NICOLE KAU, SBN 292026
ELIZABETH K. WATSON, SBN 295221
Deputy Attorneys General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3847
E-mail: Elizabeth.Watson@doj.ca.gov
Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, LLC d/b/a NetChoice, **Plaintiff,** **v.** **ROB BONTA, ATTORNEY GENERAL OF THE STATE OF CALIFORNIA, in his official capacity,** **Defendant.**	5:22-cv-08861 **DECLARATION OF EMILY KEANEY, DEPUTY COMMISSIONER OF REGULATORY POLICY FOR THE INFORMATION COMMISSIONER'S OFFICE IN SUPPORT OF DEFENDANT'S OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION**

I, Emily Keaney, declare and state as follows:

1. I am Deputy Commissioner (Regulatory Policy) for the Information Commissioner's Office. The Information Commissioner's head office is Wycliffe House, Water Lane, Wilmslow, Cheshire, United Kingdom SK9 5AF. I am responsible for overseeing the ICO's policy work programme, both domestically and internationally. I provide oversight for the work of the Information Commissioner's Office economic analysis directorate and oversee work in responding to and preparing for major legislative change. I am providing this declaration in support of Defendant's Opposition to Plaintiff's Motion for Preliminary Injunction to explain the basis on which the ICO adopted the Age Appropriate Design Code (commonly referred to as the "Children's Code") in the UK and how it has been implemented in practice. I make this declaration from personal knowledge and a review of the Information Commissioner's Office's records kept in the ordinary course of business.

BACKGROUND ON THE INFORMATION COMMISSIONER'S OFFICE

2. The role of the Information Commissioner is that of a corporation sole[1] and is currently occupied by John Edwards, who was appointed in January 2022. The Information Commissioner's Office is a non-governmental public body which is made up of officers and staff appointed by the Commissioner[2]. All formal powers and duties rest with the Commissioner. For the purposes of this statement, where I reference the ICO, this will include reference to the Information Commissioner and the Information Commissioner's Office.

3. The ICO is the regulator for data protection[3], e-privacy[4], freedom of information[5] and a number of other digital regulatory areas[6].

---

[1] Data Protection Act 2018, Schedule 12, para 1(1)

[2] Data Protection Act 2018, Schedule 12, para 5

[3] Data Protection Act 2018 and The United Kingdom General Data Protection Regulation (UK GDPR)

[4] The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

[5] The Freedom of Information Act 2000 (FOI)

[6] The ICO has additional duties and powers in respect of the following: The Environmental Information Regulations 2004, INSPIRE Regulations 2009, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing

4. Whilst the ICO is an independent regulator, it is accountable to the UK Parliament and the public for the outcomes it achieves. The Department for Science, Innovation and Technology is the ICO's sponsoring department within the UK Government.

THE DATA PROTECTION REGIME IN THE UK

5. The Data Protection Act 2018 (DPA2018), the United Kingdom General Data Protection Regulation (UKGDPR) and the Privacy and Electronic Communications Regulations 2003 (PECR) form the key data protection legislation within the UK.

6. The UK GDPR is derived from European Union (EU) law, having been retained[7] and amended[8] in UK law during the process of the UK leaving the EU, commonly known as "Brexit". The DPA2018 (DPA), which sits alongside the UK GDPR, sets out the regulatory regime for data protection within law enforcement[9] and intelligence services[10]. The DPA2018 also builds upon the obligations under the UK GDPR, which provides the Information Commissioner with specific information gathering and enforcement powers to carry out his role, and sets out the process under which the Commissioner is appointed as the UK data protection regulator[11].

7. PECR sets out legal requirements covering a number of areas, as follows:

- Marketing by electronic means, including marketing calls, texts, emails and faxes.
- The use of cookies or similar technologies.
- Security of public electronic communications services.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

Directive 1999/93/EC (eIDAS), the Re-use of Public Sector Information Regulations 2015, The Network and Information Systems Regulations 2018, and the Investigatory Powers Act 2016

[7] The European Union (Withdrawal) Act 2018, s2

[8] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

[9] The Data Protection Act 2018, Part 3

[10] The Data Protection Act 2018, Part 4

[11] The Data Protection Act Part 5, s114 and Schedule 12

8. In order to understand how the Children's Code operates and its status under UK law, it is important to explain the underlying law on which it is based. In that regard, the UK GDPR sets out the main substantive provisions of data protection law that applies in the UK. The UK GDPR applies to the processing of personal data in two ways:

- personal data processed wholly or partly by automated means (that is, information in electronic form); and
- personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).[12]

9. The UK GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.[13]

10. Article 5(1) of the UK GDPR sets out 'data protection principles' to ensure that personal data is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Under Article 5(2) of the UK GDPR it is for the data controller to demonstrate compliance with the above principles and this is called the accountability principle.

11. Chapter III of the UK GDPR also gives rights to individuals in respect of their personal data. These include the right for individuals to:

- be informed about how their data is being used

[12] Art 2(1) UK GDPR
[13] Art 2(2) UK GDPR

- access their personal data
- have incorrect data updated
- have their personal data erased
- stop or restrict the processing of their personal data
- data portability (allowing individuals to obtain and reuse their personal data for different services)
- object to how their data is processed in certain circumstances

12. The UK GDPR also sets out rights for individuals when an organisation is using personal data for automated decision-making processes (without human involvement) and profiling (Article 22).[14]

13. Under the UK GDPR children warrant special protection in how their personal data is used. This reflects Recital 38 of the UKGDPR, which states:

> "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

14. The ICO enforces the UK GDPR, DPA 2018 and PECR through a variety of regulatory interventions. These range from providing guidance and tools to signal clear expectations and to empower responsible personal data use, through to issuing enforcement notices and monetary penalties, where it is necessary to do so. The ICO's interventions aim to create a fairer playing field for compliant organisations and to protect individuals. Further details

[14] 'Profiling' is defined in Article 4(4) UK GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

relating to the way in which the ICO uses enforcement powers can be found in the ICO's Regulatory Action Policy.

Territorial scope of the UK GDPR

15. Article 3 of the UK GDPR sets out the territorial scope of the UK GDPR. The UK GDPR applies to organisations which have an establishment in the UK and also to organisations based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK (irrespective of whether a payment is required); or
- monitoring the behaviour of individuals so far as that behaviour takes place in the UK.

THE CREATION & APPLICABILITY OF THE CHILDREN'S CODE

Section 123 of the Data Protection Act of 2018

16. Under s123(1) of the DPA 2018, the ICO is required to produce a code of practice "on standards of age appropriate design of relevant Information Society Services which are likely to be accessed by children".

17. Under s123(7) DPA 2018 the following definitions apply:

- "age-appropriate design" means the design of services so that they are appropriate for use by, and meet the development needs of, children;
- "information society services" has the same meaning as in the UK GDPR, but does not include preventive or counselling services;
- "relevant information society services" means information society services which involve the processing of personal data to which the UK GDPR applies;
- "standards of age-appropriate design of relevant information society services" means such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children.

The Applicability of the Children's Code to Information Society Services

18. An information society service (ISS) is defined in the UK GDPR by reference to the definition under EU law and means any service:

- normally provided for remuneration;
- at a distance;
- by electronic means; and
- at the individual request of a recipient of services.[15]

19. The Children's Code is clear that this is a broad definition, meaning that most online services are ISS and fall within the scope of the Children's Code. This includes apps, programs and many websites, such as search engines, social media platforms, online messaging or internet based voice telephony services, online marketplaces, content streaming services, online games, news or educational websites, and any websites offering other goods or services to users over the internet. Electronic services for controlling connected toys or other devices are also ISS. [16]

20. Services that are outside the scope of the Children's Code include some services provided by public authorities, so long as these services are not typically offered on a commercial basis. Websites that only provide information about a real-world business but do not allow customers to buy products are also out of scope of the Children's Code. Traditional voice telephony and general broadcast services, such as scheduled television and radio transmissions aired to a general audience are not relevant ISS, although if a service offers both general broadcast and on demand services then the latter will be covered by the Children's Code. Finally, the Children's Code does not apply to websites or apps offering online counselling or preventive services to children.[17]

21. The Children's Code will only apply where the provision of the ISS involves the processing of personal data to which UK GDPR applies.

[15] See Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, 9 September 2015.

[16] Information Commissioner's Office. Age appropriate design code: services covered by the code, 2 September 2020, p.16.

[17] Information Commissioner's Office. Age appropriate design code: services covered by the code, 2 September 2020, p.16 and 17.

22. When the Children's Code refers to services that are "likely to be accessed by children", this means services that are:

- intended for use by children; **or**
- not specifically aimed or targeted at children, but are nonetheless likely to be used by under 18s.[18]

23. Even if an ISS states in its terms of service that under 18s should not access the service, the site will still fall within scope of the Children's Code if children access it in practice.[19]

The Definition of "Children" under the Children's Code

24. In preparing the Children's Code, the Commissioner was required to consider the UK's obligations under the United Nations Convention on the Rights of the Child (UNCRC), and the fact that children have different needs at different ages. [20] A child is defined in the UNCRC and for the purposes of this code as a person under 18 years of age.

25. In particular, the Children's Code aims to ensure that online services use children's data in ways that support the rights of the child to:

- freedom of expression;
- freedom of thought, conscience and religion;
- freedom of association;
- privacy;
- access information from the media (with appropriate protection from information and material injurious to their well-being);
- play and engage in recreational activities appropriate to their age; and
- protection from economic, sexual or other forms of exploitation.[21]

The Legal Status of the Children's Code

[18] Information Commissioner's Office, Age Appropriate Design Code: Services covered by the code, 2 September 2020, p.17.

[19] ICO consultation on the draft guidance for 'Likely to be accessed' in the context of the Children's Code | ICO, 24 March 2023.

[20] The Data Protection Act 2018, s123(4)

[21] Information Commissioner's Office. Age appropriate design code: standard 1 best interest of the child, 2 September 2020, p.24.

26. The Children's Code is a statutory code of practice; it was laid before Parliament on 11 June 2020 and issued on 12 August 2020 under section 125 of the DPA 2018. It came into force on 2 September 2020, with a 12 month transition period, meaning organisations were given 12 months to bring their services into compliance.

27. The Children's Code does not constitute new law and does not itself impose any legal obligations. Instead it explains how relevant organisations should apply the existing requirements set out in the UKGDPR, the DPA 2018 and PECR. In that regard, it should be noted that the DPA 2018 is clear that "A failure by a person to act in accordance with a provision" of the Children's Code "does not of itself make that person liable to legal proceedings in a [UK] court or tribunal."[22]

28. However, the Children's Code does have some legal force. Under section 127 of the DPA 2018, the Commissioner must take the Children's Code into account when considering whether an online service has complied with its data protection obligations under the UK GDPR, DPA 2018 or PECR. The Children's Code is clear that the "Commissioner will take the Children's Code into account when considering questions of fairness, lawfulness, transparency and accountability"[23] under the UK GDPR.

29. Furthermore, in respect of any proceedings before the UK courts or tribunal, the provisions of the Children's Code must be taken into account by the court or tribunal where relevant "in determining a question arising in the proceedings"[24].

30. It should be noted that the DPA 2018 is clear that "A failure by a person to act in accordance with a provision" of the Children's Code "does not of itself make that person liable to legal proceedings in a court or tribunal."[25] Therefore enforcement action will only occur where there is underlying infringement or breach of the UKGDPR, the DPA 2018 or PECR.

[22] S127(1) DPA 2018

[23] Information Commissioner's Office. Age appropriate design code: standard 1 best interest of the child, 2 September 2020, p.12.

[24] S127(4) DPA 2018

31. The ICO is clear that online services intended for adult audiences but likely to be accessed by a significant number of children need to take a risk based and proportionate approach by either:

- applying the standards of the Children's Code to all users; or
- reducing access to the service by children (e.g. by using user experience design measures or age assurance systems) so that children no longer represent a significant number of users.[26]

ABOUT THE UK CHILDREN'S CODE

32. The Children's Code (attached as Exhibit A) sets out 15 standards of age appropriate design that companies need to implement to ensure their services appropriately safeguard children's personal data and process children's personal data fairly (and thereby comply with UK data protection law). These are as follows:

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. **Data protection impact assessments (DPIAs)**: Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.[27]
3. **Age appropriate application**: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that

[26] Information Commissioner's Office. Age appropriate design code: services covered by the code, 2 September 2020, p.18. and 'Likely to be accessed' by children – FAQs, list of factors and case studies | ICO – Note this is currently in draft form and out for consultation.

[27] Article 36 of the UK GDPR requires controllers to carry out an assessment of the impact of the envisaged processing operations where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons (taking into account the nature, scope, context and purposes of the processing).

is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.

4. **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.
5. **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 UK Government advice.
6. **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).
7. **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).
8. **Data minimisation**: Collect and retain only the minimum amount of personal data you need 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.
9. **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.
10. **Geolocation**: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). 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.

11. **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.
12. **Profiling**: Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, 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).
13. **Nudge techniques**: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.
14. **Connected toys and devices**: If you provide a connected toy or device ensure you include effective tools to enable conformance to this code.
15. **Online tools**: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.[28]

33. The Children's Code takes a privacy by design approach, consistent with Article 25 of the UKGDPR, and is reflective of the data protection principles in UK GDPR. It provides guidance on the areas that ISS must consider to ensure their services comply with the legislation. The Children's Code states: 'If you don't conform to the standards in this code, you are likely to

[28] Information Commissioner's Office. Age appropriate design code: code standards, 2 September 2020, p.6.

find it more difficult to demonstrate that your processing is fair and complies with the GDPR and PECR. If you process a child's personal data in breach of the GDPR or PECR, we can take action against you.'[29]

34. When devising the Children's Code the ICO undertook a public consultation with a wide range of stakeholders, including industry bodies, online services, child advocacy groups and civil society organisations and, importantly, children and parents themselves. The ICO published a summary and response to the consultation[30] and the final version of the Children's Code reflected significant changes to clarify a range of areas, including age assurance.

SUPPORTING BUSINESSES TO CONFORM WITH THE CHILDREN'S CODE

35. The ICO has published a range of guidance and tools to support organisations in complying with the Children's Code and the underlying data protection legislation. The guidance is designed to improve regulatory certainty and support businesses to implement privacy by design practices.

36. Although the standards in the Children's Code are themselves a 'how to' guide, this is also supplemented by detailed guidance on the ICO's Children's code hub page.[31] ISS can then link to guidance available on the wider ICO website to address core data protection principles[32] and more detailed guidance such as our data sharing code of practice[33] and guidance on creating Data Protection Impact Assessments (DPIAs).[34]

The Commissioner's Opinion on Age Assurance

37. Standard 3 of the Children's Code relates to age appropriate application:

> "Standard 3: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either

---

[29] Information Commissioner's Office. Age appropriate design code: about this code, 2 September 2020, p.12.

[30] Information Commissioner's Office. Consultation on Age appropriate design: a code of practice for online services Summary of responses, 17 January 2021 <https://ico.org.uk/media/about-the-ico/consultations/aadc/2616996/summary-of-responses.pdf>

[31] Children's Code: additional resources | ICO

[32] Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

[33] Data sharing information hub | ICO

[34] Data protection impact assessments | ICO

establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead."[35]

38. During the transition period for the Children's Code, stakeholders requested more clarity from the ICO on the approach to age assurance in relation to Standard 3. In 2021, the Commissioner's Opinion on age assurance was published which set out expectations for complying with standard 3.[36] This Opinion explains how age assurance can form part of an appropriate and proportionate approach to reducing or eliminating risks and complying to the Children's Code.

39. Since publishing the opinion, the ICO has continued to engage with industry to further support the adoption of appropriate, accurate and efficient approaches to age assurance, including:

- Research to develop the ICO's understanding of the risks to children across different types of ISS, their varying functionality and their processing of personal data[37].
- Developing the ICO's understanding of how ISS are currently assessing these risks, and identify good practice and opportunities for improvement.[38]
- Developing the ICO's understanding of the available and appropriate mitigations to respond to these risks, and specifically when and what kind of age assurance is likely to be appropriate and proportionate.
- Supporting the development of international age assurance standards through IEEE[39] and ISO[40] standards.

Children's Code Guidance Products

[35] 3. Age appropriate application | ICO
[36] ICO (2021) Information Commissioner's opinion: age assurance for the Children's Code. Available at: https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf (Accessed: 21 February 2023).
[37] Findings from two research reports are available at: Age Assurance research | ICO
[38] See Children's Code Self-Assessment Risk Tool | ICO
[39] IEEE SA - Children's Data Governance
[40] Standards for Age Verification | AVPA (avpassociation.com)

40. The ICO has produced guidance products that sit alongside the Children's Code to assist organisations in their compliance with the Children's Code. Details of these products are provided below.

41. Any further reading or other resources which are mentioned in or linked from the Children's Code do not form part of the Children's Code. There is no statutory obligation under the DPA 2018 for the ICO or courts to take the guidance into account (unless it is another separate statutory code of practice).[41]

42. To support the adoption of privacy by design practices that protect children's data, the ICO developed Children's Code design guidance targeted at businesses' user experience design teams. This was well received by the intended audience and won the Design for Good award 2022 from the Institute of Designers Ireland[42]. A conformance testing tool has also been created to allow designers to test their product ideas against the Children's Code.

43. The ICO received feedback from industry that the principle of the 'best interest of the child' was new to some business, which might lead to uncertainty in how to comply with Standard 1 of the Children's Code. The ICO developed a best interest framework to help business conduct a balancing test on risks and opportunities of their online service to determine if they are in compliance with the best interest standard and children's rights under the UN Convention on the Rights of a Child.

44. The ICO has developed a Children's Code self-assessment tool for industry to help them carry out their own risk assessment of their online service in the context of the UK GDPR and the Children's Code. This toolkit provides them with examples of the practical steps that can be taken to ensure the best approach is adopted to safeguard children's privacy and ensure compliance to the 15 standards of the code.

45. Standard 3 of the Children's Code states that services targeted at children, or which feature high risk processing, must complete a DPIA. To support industry to comply with this standard, the ICO has developed tools for completing DPIAs, and three sample DPIAs for

[41] Information Commissioner's Office. Age appropriate design code: about this code, 2 September 2020, p.13

[42] ICO - Children's Code design guidance - IDI Awards

providers of mobile games or apps, online retail services and connected toys (attached as Exhibits B1, B2, and B3, respectively).

46. The Children's Code is focused on the ICO's regulatory remit of data protection and e-privacy. Standard 5 of the Children's Code states that businesses should not use data to deliver content that is detrimental to children. However, the ICO is not a content regulator and therefore the guidance in the Children's Code focuses on established UK government or industry guidance and standards (e.g. advertising standards) about what is considered to be detrimental to children. The ICO is focused on how the content is delivered through the processing of personal data, not the nature of the content. The ICO has produced guidance that collates sources of guidance from other organisations about protecting children's wellbeing to support ISS in assessing if they are processing data in a way that could detrimentally impact children.

47. The ICO has produced sector specific guidance for the games industry and providers of educational technology addressing compliance questions that specifically arise in the context of these sectors.

48. In addition to these guidance products that relate specifically to the Children's Code, the ICO also has other statutory codes of practice and a wide range of other guidance that helps businesses comply with UK data protection legislation. This guidance covers a range of related topics, including:

- Overview of Data Protection Harms and the ICO's Taxonomy
- Examples of processing 'likely to result in high risk'
- Data sharing code of practice
- Privacy notice templates
- Direct marketing guidance
- Data protection impact assessments

Certification Schemes

49. Under UK GDPR, the ICO may approve certification schemes that provide assurance that a service meets an appropriate set of data protection standards.[43] Compliance with a certification scheme is therefore a way for an organisation to demonstrate compliance with UK GDPR.

50. The ICO has issued detailed guidance in respect of certification, which explains that:

> "Certification is a way of demonstrating that your processing of personal data complies with the UK GDPR requirements, in line with the accountability principle. Certification can help demonstrate data protection in a practical way to businesses, individuals and regulators."

51. There have been four certification schemes approved by the ICO to date, and two of these relate to children's privacy:

- The Age Check Certification Scheme;[44] and
- The Age Appropriate Design Certification Scheme.[45]

52. As of February 2023, five organisations have received certification under these schemes and others are progressing through the process. The schemes are based on UK data protection law and the standards set out in the Children's Code.

SUPERVISION OF THE CHILDREN'S CODE

53. The ICO monitors compliance with the Children's Code using the full range of measures available and takes regulatory action where appropriate and proportionate.

54. The ICO's approach is to encourage compliance. Where non-compliance is identified the ICO takes fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected. In deciding whether to

[43] Articles 42 and 43 UK GDPR make provision for certification. The Commissioner's powers to accredit certification bodies and approve criteria of certification are set out in Article 58(3) UK GDPR.

[44] ICO (2021) Age Check Certification Scheme. Available at: https://ico.org.uk/for-organisations/age-check-certification-scheme-accs/ (Accessed: 27 February 2023).

[45] ICO (2021) Age Appropriate Design Certification Scheme. Available at: https://ico.org.uk/for-organisations/age-appropriate-design-certification-scheme-aadcs/ (Accessed: 27 February 2023).

take regulatory action against an organisation, the ICO takes account of a range of factors, including the size and resources of the organisation concerned, the availability of technological solutions in the marketplace, and the risks to children that are inherent in the processing. The ICO takes a proportionate and responsible approach, focusing on areas with the potential for most harm and selecting the most suitable regulatory tool.[46]

55. The ICO has identified three sectors where children access services in large numbers, and where there is likely to be the greatest risks of harm to children. These are online games, social media, and streaming services.

56. Having identified these sectors as priorities for supervision, the ICO asked over 50 organisations to respond to questions about the steps they had taken to implement the Children's Code. The responses received provided an insight into the steps taken and to what extent the organisations had started to build compliance with the Children's Code into the operation of their businesses.

57. Based on this work, the ICO considers that the provisions of the UK GDPR that are the most likely to be infringed as a result of non-compliance with the Children's Code include:

- Article 5(1) UK GDPR, which requires personal data to be processed lawfully, fairly and in a transparent manner.
- Article 8 UK GDPR, which requires that where an ISS is offering a service directly to a child under the age of 13 and seeks to rely on consent as the lawful basis for processing, this consent must be provided by a parent.
- Articles 5(1)(c) and (f) UK GDPR, which respectively relate to data minimisation and data security.

ICO Children's Code Audits

58. The ICO has conducted ten audits of organisations under the Children's Code. As set out in the ICO's guidance, Children's Code audits typically assess the organisation's procedures, systems, records and activities in order to:

[46] Regulatory Action Policy (ico.org.uk), pg.3

- ensure that appropriate policies and procedures are in place;
- verify that those policies and procedures are being followed;
- test the adequacy of controls in place;
- detect breaches or potential breaches of compliance; and
- recommend any required changes in control, policy and procedure.[47]

59. The scope of the Children's Code audits carried out by the ICO to date covered some of the following areas:

- governance, transparency and rights;
- diligence and DPIAs;
- minimisation and sharing;
- age assurance;
- detrimental use;
- privacy settings and parental controls;
- geolocation;
- profiling and cookies;
- nudge techniques;
- connected toys and devices; and
- AI & online services.[48]

60. Following the audit, the organisation that has been audited is provided with a report setting out the findings of the audit. A non-confidential summary of the audit is also published on the ICO's website.[49] To date, summaries of six Children's Code audits have been published. These summaries provide similar organisations with an insight into the ICO's expectations regarding compliance with the Children's Code.

61. Following audits of video game design companies, the ICO has produced "top tips" for assisting game designers in complying with the Children's Code.[50]

[47] See a-guide-to-audits-for-the-age-appropriate-design-code.pdf (ico.org.uk)
[48] Note that each audit covered three to four of these areas.
[49] See Audits and overview reports | ICO for Children's Code related audit reports.
[50] Top tips for games designers – how to comply with the Children's Code | ICO

Engagement

62. The ICO regularly engages with ISS to support their compliance with the Children's Code. Informal feedback to businesses has involved explaining best practice about how organisations handle children's data, including through the use of additional prompts and reminders to users, increased parental controls, and the implementation of family management tools.

63. The ICO also undertook a number of workshops which ISS could apply to attend – these have taken place between 2020 and 2022 and provided an introduction to the Children's Code, with some workshops focussing on "best interests of the child", "risk assessment" and "likely to be accessed guidance".

64. In April 2021 the ICO issued a "transparency champions open call" where participants in the open call were invited to submit ideas and examples of privacy information designs that meet the vision of the Children's Code transparency standard. In June 2021 the ICO issued Insights from the Children's Code transparency champions open call, outlining the findings of the review highlighting thematic areas of good practice.

IMPACT OF THE CHILDREN'S CODE

65. The Children's Code has had a significant impact on how ISS process and protect children's data, with changes already announced by large digital economy companies. For example:

- Google pledged to turn location history off for all users under the age of 18 globally, without the option to turn it on[51].
- Google produced resources to help children, young people and their parents to help them better understand its data practices[52].
- Meta has limited personalised advertising to age and location for users under 18[53].

[51] Giving kids and teens a safer experience online (blog.google)
[52] Giving kids and teens a safer experience online (blog.google)
[53] Age appropriate ads for teens - Meta

- Meta has introduced privacy by default settings for teen users of Facebook and Instagram. It is also developing online tools to safeguard teen users[54].
- Meta is testing ways to verify the ages of users on Instagram in situations where users attempt to edit their age from under the age of 18 to over the age of 18. Options currently being tested include ID verification and video selfie verification.[55]
- Snap has launched a digital literacy programme aimed at educating users about data, privacy and online safety; it has removed browsable public profiles for under 18s; and has set default chat functions to friends only.[56]
- Snap has launched a 'Family Centre Hub' which includes parental control features.[57]
- TikTok has removed messaging for users under 16[58] .
- Twitter now requires users to enter their date of birth. Previously, Twitter grouped adults and children in the same categories for targeted advertising purposes.
- Epic Games has introduced improved parental control tools and "Cabined Accounts"[59] so that children under the age of 13 do not have their personal data processed until verifiable parental consents[60] have been obtained.
- Epic has partnered with LEGO[61] to create safe digital play spaces and has committed to safeguard children's privacy by putting children's best interests first.
- Roblox has introduced improved parental control tools and simplified transparency information[62].

[54] Protecting teens and their privacy on Facebook and Instagram - Meta
[55] New ways to verify age on Instagram - Meta
[56] https://values.snap.com/en-GB/news/data-privacy-day-supporting-the-privacy-and-wellbeing-of-snapchatters
[57] Family Centre - Parental Control For Teens | Snapchat Safety
[58] TikTok: Under 16s can no longer use direct messaging - BBC Newsround
[59] Introducing Epic Games cabined accounts
[60] Parental controls - Epic Games
[61] The LEGO Group and Epic Games Team Up to Build a Place for Kids to Play in the Metaverse - Epic Games
[62] Age Appropriate Design Code FAQs – Roblox Support

66. The ICO conducted three rounds of research with ISS in scope of the Children's Code covering the 2020-2022 period to track the impact of the Children's Code. The last round of research was conducted in the autumn of 2022, one year after the Children's Code entered into its supervision phase (results attached as Exhibit C). Key findings related to business include:

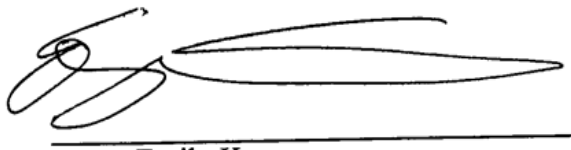
- Businesses felt the overall impact of the Children's Code would be positive for wider stakeholders. Around three quarters (77%) of businesses (2022 wave) thought there would be a positive impact on parents/guardians and 71% thought it would be beneficial for children. Two thirds (66%) thought it would be positive for their organisation and 63% felt it would have a positive impact on their sector (there was no notable difference in this figure across sectors).
- Three quarters of businesses understand the theory within the Children's Code (72%) and understand what conformance with the Children's Code requires (74%).
- Fewer businesses reported that they incurred costs because of the Children's code in 2022 than in 2021 (29% compared with 35%). As in previous years, smaller companies were less likely to have incurred costs from the Children's Code (6% sole trader, 14% micro, 19% small, 45% medium, 33% large), which was driven by a lower proportion thinking that they are in scope.
- The proportion of businesses that recently incurred costs has also fallen because changes had already been made as businesses move towards conformance over time.
- As in autumn 2021, businesses were more likely to think that they were in scope prior to hearing a definition of the Children's Code, something that was consistent in 2022. Although fewer businesses thought they were in scope in 2022 than in 2021 (81% vs 84%) and slightly more thought they were after the definition (73% vs 68%) these differences were fairly minor.
- Between 2021 and 2022 there was no significant change in the proportion of businesses that consider themselves fully conformant with the Children's Code: 44% of businesses reported this in 2021 and 46% in 2022.

- Ease of being conformant remains consistent with 2021, with just over a fifth (21%) of businesses finding it difficult to be conformant with the Children's Code, but micro business were far less likely to find this (9%) and medium sized businesses were more likely to find it difficult (42% reported this).
- Businesses were generally more likely to have made these changes regardless of the Children's Code. For example, 52% made changes in designing and implementing changes to aspects of the service's user experience independently of the Children's Code compared with 35% who made the change as a direct result of the Children's Code.
- Very few businesses find it difficult to conform with the Children's Code, it tends to be perceived as integrated into the general data protection conformance of the business. Challenges were more often faced by smaller businesses than large businesses.
- While more businesses reported incurring costs in the highest bracket compared to 2021, only a minority stated the costs were directly related to the Children's Code. In general, the number of businesses experiencing costs had fallen, showing no detrimental impact to businesses.

67. In September 2022, John Edwards confirmed that the ICO has "seen real changes since the Children's Code came into force a year ago. These changes come as a result of the ICO's action enforcing the Children's Code, making clear to industry the changes that are required."[63] The ICO continues to work with industry, civil society groups, parents and children to build upon compliance with the Children's Code and the underlying data protection legislation.

[63] "Children are better protected online in 2022 than they were in 2021" - ICO marks anniversary of Children's Code | ICO

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on 19th April 2023, at London, United Kingdom.



Emily Keaney
Deputy Commissioner (Regulatory Policy)
Information Commissioner's Office