Title: Age Appropriate Design Code **Lead department or agency:** Information Commissioner's Office /DCMS **Other departments or agencies: N/A**	Impact Assessment (IA)
	Date: 3/07/2020
	Stage: Final
	Source of intervention: Legislative
	Type of measure: Statutory Code of Practice
Summary: Intervention and Options	

What is the problem under consideration? Why is regulatory action or intervention necessary?

The Information Commissioner was required to prepare the Age Appropriate Design Code (the code) by Parliament under s123 of the Data Protection Act 2018 (DPA 2018) in order to address risks in the use of children's personal data by online services, and resulting harms to children. Parliament deemed that specific regulatory intervention was necessary because, particularly in the context of wider online harms, self-regulation of age appropriate design had proved to be ineffective.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

As the code and its remit was mandated by Parliament in s123 DPA 2018 it was not appropriate for the Commissioner to consider any alternative course of action. Further background to the scope of the code is available in the accompanying Explanatory Memorandum published alongside the code.

To the extent that the Commissioner had discretion about which issues to cover or how to interpret them within the code, these are described in the body of this assessment.

Will the policy be reviewed?

The Commissioner has committed to reviewing how effectively the code is working and whether the costs and benefits are in line with expectations one year after the end of the transition period. This is in line with standard good regulatory practice. We would expect the review to start in the Autumn of 2022.

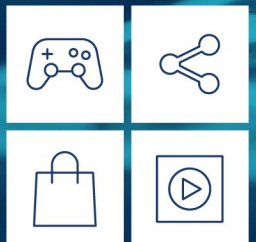
Information Commissioner's Office

Age appropriate design: a code of practice for online services

Impact assessment

ico. Information Commissioner's Office

children's code



Contents

1. Executive summary 4
2. Background 9
   - 2.1 Problem under consideration 9
   - 2.2 Rationale for intervention 13
   - 2.3 High level policy objectives 14
   - 2.4 Approach to the code 16
   - 2.5 Scope of the code 16
   - 2.6 Affected groups 17
   - 2.7 Principles and approach 19
   - 2.8 Regulatory constraints 21
3. Cost benefit analysis 23
   - 3.1 The scope of the code 24
   - 3.2 Standard 1 – the need to consider the best interests of children 29
   - 3.3 Standard 2 –the need to undertake a data protection impact assessment (DPIA) 32
   - 3.4 Standard 3 – The need to establish the age of individual users with an appropriate level of certainty 35
   - 3.5 Standard 4 – the need to provide age appropriate privacy and other information 39
   - 3.6 Standard 5 - the need to establish when use of data may have a detrimental effect on children and to design services so that data is not used in this way 41
   - 3.7 Standard 6 – the need to uphold own published terms, policies and community standards 45
   - 3.8 Standard 7 – the need to provide high privacy settings by default 46
   - 3.9 Standard 8 - the need to minimise the collection and retention of personal data 50
   - 3.10 Standard 9 – the need to only share children's personal data if there is a compelling reason to do so 51
   - 3.11 Standard 10 – the need to switch geolocation options off by default, provide a sign when location tracking is active, and default options which make a child's location visible to others off at the end of each use 53

3.12 Standard 11 – the need to ensure that when parental controls are provided children get an obvious sign that their online activity is being monitored..... 55

3.13 Standard 12 - the need to switch options which rely upon profiling off by default and to only allow profiling if suitable measures are in place to protect children from harmful effects..... 56

3.14 Standard 13 – the need to avoid the use of nudge techniques to encourage children to provide unnecessary data or lower privacy settings 58

3.15 Standard 14 – the need to ensure that connected toys and devices comply with the requirements of the code 60

3.16 Standard 15 – the need to provide age appropriate online tools 61

1. Executive summary

Today's children spend more time online than ever before, and the current Covid-19 pandemic has only exacerbated this trend. The internet offers huge opportunities, but many of the sites and services children are using have not been designed with them in mind. This can pose risks to children: risks to their privacy and, potentially, risks to their emotional or physical wellbeing if their data is processed in ways that expose them to harm.

To address these risks, the UK Parliament directed the Information Commissioner (the Commissioner) to produce a statutory Code of Practice, through the provision in s123 of the Data Protection Act 2018 (DPA 2018). The code is a tool to steer businesses to comply with the existing legislation.

This impact assessment sets out the benefits and costs associated with the resulting Age Appropriate Design Code (the code) produced by the Commissioner and laid before Parliament on 10 June 2020.

The final version of the code reflects significant changes in response to our consultation with stakeholders, including with industry bodies, child advocacy groups and civil society organisations and, most importantly, children and parents themselves. We have drawn evidence from the consultation, and publicly available research and data, to create this impact assessment.

The Commissioner acknowledges the importance of conducting impact assessments as regulatory good practice, in appropriate circumstances. She also recognises the benefit of using this impact assessment to inform the next stages of the work to implement the code.

Parliament set the scope of the code so it would be broad, covering not just online services designed for children but also those services that are likely to be accessed by children. It puts the onus on businesses to ensure those services have age-appropriate data protection in place, shifting the burden from sitting solely with children and parents.

Benefits

Protecting vulnerable citizens and supporting economic growth, including for small businesses, are two of the ICO's main priorities. Once the code is in place, 14.2 million UK children are set to benefit from the higher privacy standards and associated reduction in online risk. It will give

confidence to up to 15.6 million parents and adults with parental responsibility, reducing the burden of anxiety and oversight knowing that these services are designed with children's privacy in mind.

It will also bring benefits to innovative UK businesses designing new solutions and services to help ensure children's privacy is built into online services, stimulating demand for their products.

The code brings more benefits to businesses by providing clarity and greater certainty about the outcomes the Commissioner expects and offers further guidance on how to achieve them.

We remain open to receiving further quantitative evidence from organisations on the costs as the implementation period progresses. We will also consider more targeted work to understand the costs and benefits where this is proportionate and will support our regulatory approach or ability to tailor the package of support.

Costs

This impact assessment builds on that conducted for the DPA 2018.[1] However, the way the broad scope has been set for the code is unique and breaks new ground for legislation covering digital services; there is no clear evidence or source to rely on to provide a definitive indication of the number of businesses covered.

We have therefore based our assessment on the DCMS's calculations of the number of businesses within scope of the proposed online harms regime. On this basis, around 290,000 businesses fall within scope of the code, though the extent to which these businesses will need to make changes to conform will depend on the level of risk the processing activities within their services pose to children. The Commissioner remains open to working with government to further review the number of affected businesses once the code is in effect, if additional evidence becomes available.

Most of the analysis in this assessment has focused primarily on non-monetised impacts, supporting these with evidence, including quantitative evidence where this has been possible.

[1] As noted in section 11 of the Explanatory Memorandum to the code, an impact assessment was produced for the Data Protection Bill which implemented the obligations of the EU GDPR in the United Kingdom: https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020

However, a total one-off cost of £60m is estimated for businesses affected by the code to familiarise themselves with the legislation, or around £2 for each of the affected children, parents and adults with parental responsibility noted above.

This cost is attributable to the s123 requirement on the Commissioner to produce a code. As part of developing the code and to minimise this cost, the Commissioner sought to ensure maximum clarity and readability while still providing the necessary information.

It is important to note that the code does not constitute new law. It is rooted in the DPA 2018, the General Data Protection Regulations (GDPR) and the Privacy and Electronic Communications Regulations 2003 (PECR) and sets out high level requirements that organisations offering information society services likely to be accessed by children should meet to comply with these requirements.

We have identified the incremental impacts the Commissioner considers can be attributed directly to the code. These occur where the code provides more specificity about how organisations should comply than exists in the GDPR and where the obligation is not an inevitable consequence of s.123 of the DPA 2018. The Commissioner finds that there is a distinct incremental impact arising entirely, or in part, from a number of standards within the code. This includes:

- some additional expectations around data protection impact assessments (DPIAs), including the costs to businesses of some extra consideration, as part of their DPIA, of how they meet the standards in the code;
- a cost in ensuring providers of information society services (ISS) identify and, where appropriate, take into account relevant voluntary industry codes to help ensure data is not used in ways that are detrimental to children;
- a cost in providers of ISS ensuring they uphold their own policies and community standards, when they do not already do so, to ensure data processing is fair and used in line with user expectations;
- a cost in reconfiguring default settings to high privacy by default, where this is not prescribed by the existing legislation on behavioural advertising (which requires users to opt in);

- a cost in reconfiguring services to have geolocation data off for default, where this is not already required in the definition of 'location data' as defined by PECR (this is a narrower definition than geolocation data);
- where services currently use, or put in place, parental controls, costs in redesigning or designing these to provide an age appropriate sign to the child that their online activity is being monitored, where this is not already in place;
- where profiling is used for other purposes than behavioural advertising and where a lawful basis other than consent is relied upon, there are likely to be some costs associated with re-designing services so this is off by default; and
- costs of redesigning services currently using nudge techniques to encourage users, including children, to provide data or lower privacy settings.

It is relevant to note that many impacts that stakeholders have identified as being of concern are not, in fact, attributable to the code but derive from the provisions of s123 of the DPA 2018 as mandated by Parliament or the underpinning explicit requirements of the GDPR or PECR.

This specifically applies to two impacts raised by stakeholders as being of most concern because of the costs involved in making changes to bring services into conformance. Namely:

1. The impact on existing business models of not being able to process children's personal data for the purposes of behavioural advertising by default (the Commissioner considers this to be the result of applying existing explicit requirements of the GDPR and PECR).
2. The cost of providing different versions of services for users of different ages (the Commissioner considers this arises from explicit requirements of s123 of the DPA 2018).

The impacts attributable to existing legislative requirements are considered to be part of the counterfactual to this impact assessment (the baseline against which the impact of the code is measured), which the Commissioner has no discretion to amend.

The nature of the code makes quantified analysis of the costs and benefits particularly challenging. The code leaves room for interpretation, with

costs varying considerably even between small and medium enterprises (SMEs).

In addition, calculating the incremental costs of the code on the affected businesses is complex, as the nature of these costs will vary considerably depending on the sophistication and maturity of the businesses existing data protection systems and processes, the nature of the services they provide, the data processing associated with those services and the level of risk to children that processing poses.

Conclusion

On balance, having assessed the incremental costs of the code, the Commissioner considers them to be outweighed by the benefits.

However, the Commissioner recognises that businesses, particularly those with limited resources, will require further support to implement the necessary changes. The Commissioner is committed to providing a significant package of advice, guidance and support to assist providers of ISS during the implementation period. The nature of that support will be informed by the impacts identified in this impact assessment. The Commissioner also intends to work closely and collaboratively with industry so that they can further shape the form and content of that support.

The Commissioner has also committed to reviewing the code 12 months after the end of the implementation period to assess how effectively businesses have implemented the code and whether further guidance or support is required.

2. Background

2.1 Problem under consideration

The code was mandated by Parliament in s123 of the DPA 2018 in order to address concerns that children are using a wide range of online services, and that the way in which their data is used by these services is not always age appropriate and can cause harm.

The Commissioner considers that the key harms to children that can arise from the processing of their personal data online, and that therefore need to be addressed by the code, are:

- privacy intrusion (including damage to personal reputation);
- harms to children's mental and emotional health and wellbeing;
- physical harms; and
- economic harms or commercial exploitation.

2.1.1 Concerns about children's online use

According to Ofcom's Online Nation 2020 Report, 86% of 12-15 year olds expressed concerns about harms related to online content and interaction with others, while over half (58%) expressed concerns about data/privacy. Meanwhile, 76% of adults also expressed concerns about potential harms to children related to content and contact, with 79% wanting websites to do more to keep people safe online.[2]

The current global pandemic has only exacerbated these concerns, with an increase in UK network traffic of 20% in March and April, and a 50% increase in the use of education sites such as BBC Bitesize suggesting an increase in the reliance by children on digital services to stay connected and to learn.[3] There is also further international evidence of this issue in policy briefings developed by the OECD[4].

The parliamentary debate during the passage of the Data Protection Bill recognised that these services are often developed for adult users, with

[2] Online Nation 2020 Report, Ofcom, PP34-37. https://www.ofcom.org.uk/__data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf

[3] Online Nation 2020 Report, P40. https://www.ofcom.org.uk/__data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf While the data on BBC Bitesize was among adult users it is likely that this is being accessed with or on behalf of children.

[4] OECD – Combatting COVID19's effect on children https://read.oecd-ilibrary.org/view/?ref=132_132643-m91j2scsyh&title=Combatting-COVID-19-s-effect-on-children

insufficient regard for the consequences for young people. It was also noted that while parental guidance and responsibility are a key part of protecting children, many parents feel they lack the knowledge or tools to offer effective support or intervention. Baroness Kidron (CB) summarised the issues as follows:

> 'Parental responsibility and guidance can never be replaced, but if devices are portable, services are designed for adults and community rules are not upheld, then parents do not have the tools to guide children in the digital environment.'
>
> 'It is not simply about the bad things that happen. It is about abusing the entire data of a child when they are online'.[5]

Much of the research on children's online experiences supports these concerns. Ofcom's 2019 *Children's Media Use and Attitudes*[6] research found that 90% of five-15 year olds went online, ranging from 57% of three-to-four year olds to 99% of 12-15 year olds. It also showed that children often use online services whilst on the go and away from parental oversight. Smartphone ownership rises from 23% for children aged nine to 56% at age 10 and then to 94% for 15 year olds; and half of 12-15 year olds say a mobile phone is the device they 'mostly' use for going online.

2.1.2 Children's use of online services designed for adults

Whilst online services offer children a world of possibility to explore, learn and develop, they also pose significant risks because many assume their users are adults.

A report commissioned by 5Rights, *Digital Childhood- Addressing Childhood Development Milestones in the Digital Environment* found that, 'access [to the digital world] that is predicated on adult maturity provides a complex environment that often gets in the way of young people meeting their development goals'.[7] Research by Professor Sonia Livingstone, a leading expert on children's experience and behaviour online, found that "even the oldest children struggle to comprehend the

[5] https://hansard.parliament.uk/Lords/2017-11-06/debates/107E5465-94B7-4604-981C-1BC49C43FF84/DataProtectionBill
[6] Children and Parents: Media Use and Attitudes Report 2019, Ofcom. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf
7 Digital Childhood-Addressing Childhood Development Milestones in the Digital Environment, 5Rights 2017, p4

https://5rightsfoundation.com/static/Digital_Childhood_report_-_EMBARGOED.pdf

full complexity of internet data flows and some aspects of data commercialisation".[8]

Research supports the argument that many of the online services children are using are designed for adults. A 2016 CBBC study, conducted by Comres, found that 78% of 10 to 12 year-olds say they have social media accounts, despite a recommended minimum age limit of 13. Nearly half (49%) of 10-12 year olds said they had an account on Facebook, while 40% had an account on Instagram.[9] Similarly, Ofcom research in 2018 found that despite Google stating in its terms that children under 13s must use YouTube Kids, 51% of three-to-four year old and 72% of five-to-seven year-olds used the full YouTube service. Of the five-to-seven year-old children, over twice as many used only YouTube (57%) than used only YouTube Kids (25%).[10]

2.1.3 Harms associated with privacy intrusion

The ability for children to access online services in a way that protects their privacy and allows them age-appropriate control over the information they share and give away is important.

Academic research has shown that privacy is vital for child development, and that privacy-related media literacy skills are closely associated with a range of child developmental areas: autonomy, identity, intimacy, responsibility, trust, pro-social behaviour, resilience, critical thinking and sexual exploration.[11]

Children develop and shape their identities and relationships via messaging apps and video sharing platforms and express their views and opinions in online public spaces. When doing so, they should have age appropriate control over how much of themselves they share and how they present themselves to others. The potential for privacy intrusion and harm to personal reputation can arise if children share their personal data without a proper understanding of the consequences of doing so, or if settings are 'low privacy' by default.

We know parents are concerned about their children's privacy. The ICO's 2019 annual track survey ranked children's privacy second only to cyber

8 Children's data and privacy online: Growing up in a digital age, p4 http://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf
9 https://www.bbc.co.uk/mediacentre/latestnews/2016/newsround-survey-social-media
10 Research into children's content consumption, including Netflix and YouTube, Ofcom 2018, https://www.ofcom.org.uk/__data/assets/pdf_file/0015/116520/Annex-Research-Childrens-Content-Consumption.pdf
11 Peter and Valkenburg, 2011; Raynes-Goldie and Allen, 2014; Pradeep and Sriram, 2016; Balleys and Coll, 2017.

security as people's biggest data protection concern,[12] and Ofcom research in 2019 found that 'companies collecting data about what their children are doing online' was the concern cited by the largest number of parents when it comes to their children's online activity.[13]

ICO-commissioned research also found that parents and children recognise there are trade-offs between privacy and access to content and services. These trade-offs can be hard for parents to manage because children are motivated by fear of missing out and do not want privacy concerns to be a barrier to the services they can access.[14]

2.1.4 Harms to children's mental, physical and emotional health and wellbeing.

In addition to the risk to children's privacy, the ways in which children's personal data is processed can also increase their exposure to other kinds of harm. In their online harms white paper, the Government identified a range of harms, including online bullying, abuse and content that can lead to anxiety, self-harm or eating disorders. Personal data processing can lead to or exacerbate these wider harms, for instance if children's personal data is used to inform content feeds, suggest contacts, or keep children online, which could result in harm to their physical and emotional wellbeing as well as their mental health.

Inappropriate sharing or processing of children's personal data can also expose children to contact risks, where bad actors persuade children into physically risky or self-harming behaviours or reveal children's actual location. Such processing can also exploit their susceptibility to mimicking risky behaviours observed online (drinking, smoking, drug use, self-harm, suicide, dangerous pranks).

Exposing children to attention retention techniques that they don't have the developmental capacity to handle (ability to defer gratification and self-manage time spent online) may also mean they are unable to ensure a healthy balance of online and offline activities.

[12] Information Rights Strategic Plan: Trust and Confidence, p23. https://ico.org.uk/media/about-the-ico/documents/2615515/ico-trust-and-confidence-report-20190626.pdf
[13] Children and parents: Media use and attitudes report 2019, Ofcom p30. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf
[14] Towards a better digital future- Informing the Age Appropriate Design Code, ICO/Revealing Reality 2019,

2.1.5 Economic harms or commercial exploitation

The use of behavioural advertising or promotion of in-app purchases to children can also make them more vulnerable to commercial exploitation, as they do not have the same critical thinking capacity as adults to recognise and evaluate commercial practices and resist commercial pressures.

A 2016 EU study of the impact of online marketing found that children are particularly vulnerable to marketing practices in online games, mobile apps and social media sites. The study focused on marketing techniques used in 25 of the most popular online games, all of which included elements of embedded or contextual advertising. The study found that online marketing had a significant effect on children's wellbeing, including higher rates of snack consumption and increased spending on in-app purchases.[15]

Nudge techniques and micro-transactions in games and mobile applications are common. often designed to be hard for young people to resist. Techniques used include in-game currency to hide the real costs of purchases, inducements to spend, time-limited reward removals and loss aversion (where micro-purchases are used to avoid losing a game).[16] These can result in obvious direct economic harm (children spending money) but also mean children's data is used for the financial gain of a commercial enterprise with no or insufficient recompense to the child (or without the child even knowing it is happening).

2.2 Rationale for intervention

The rationale for intervention via a statutory Code of Practice was set by Parliament. It was Parliament's view that leaving matters to self-regulation is not sufficient and had previously proved ineffective.

During the debate on the Data Protection Bill Baroness Kidron (CB) argued that self-regulation had, "not provided a high bar of data protection for children." Baroness Harding of Winscombe (CON) supported this point stating that, "the truth is that some of the largest companies in the world are simply not putting in place the most basic protections for our children" and that "in research conducted by the Children's Society,

[15] Study on the impact of marketing through social media, online games and mobile applications on children's behaviour, European Commission, 2016. https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en
[16] The Rip-off Games, Parent Zone 2019. P9. https://parentzone.org.uk/the-rip-off-games

83% of children said that they think that social media companies should do more to protect them."[17]

The code's statutory footing means that when the Commissioner is carrying out any of her regulatory functions in relation to the underlying GDPR, DPA 2018 or PECR, including using any of her corrective measures, she is required to take it into account to the extent it is relevant. Courts and tribunals are also required to take the code into account to the extent it is relevant to any proceedings before them.

As the code was mandated by Parliament in s123 DPA 2018 the Commissioner did not have an option to consider alternative action or regulatory intervention.

This rationale also aligns with the direction of travel internationally, including evidence submitted to the current OECD's review of their 2012 Recommendation on the Protection of Children Online[18]

2.3 High level policy objectives

The Commissioner's high policy objectives in the drafting of the code were as follows:

- To implement the following intentions of Parliament (as set out in s123 DPA 2018) that the code should:
    - cover ISS that process personal data and are likely to be accessed by children.
    - have regard to the UK's obligations under the United Nations Convention on the Rights of the Child (UNCRC).
    - set standards of age appropriate design which are desirable having regard to the best interests of children.
    - account for the fact that children have different needs at different ages.
    - ensure that services are designed so they are appropriate for use by, and meet the development needs of, children.

[17] https://hansard.parliament.uk/lords/2017-12-11/debates/154E7186-2803-46F1-BE15-36387D09B1C3/DataProtectionBill(HL)

[18] Review of the 2012 OECD Recommendation for the Protection of Children Online https://www.oecd.org/sti/ieconomy/workshop-on-the-protection-of-children-in-a-connected-world.htm and https://www.oecd.org/sti/ieconomy/protecting-children-online.htm

- To further implement the intentions of Parliament by covering the following list of suggested areas for inclusion in the code,provided by Government,[19] as appropriate:
    - Default privacy settings.
    - Data minimisation standards.
    - The presentation and language of terms and conditions and privacy notices.
    - Uses of geolocation technology.
    - Automated and semi-automated profiling.
    - Transparency of paid-for activity such as product placement and marketing.
    - The sharing and resale of data.
    - The strategies used to encourage extended user engagement.
    - User reporting and resolution processes and systems.
    - The ability to understand and activate a child's right to erasure, rectification and restriction.
    - The ability to access advice from independent, specialist advocates on all data rights.
- To reduce harms to children that arise from the processing of their personal data online.
- To improve the current provision of ISS used by children so that children are provided with protection in how their personal data is used by default, without them (or their parents) having to take any action.
- To empower children to explore the digital environment and maximise its positive opportunities.

[19] Lord Ashton, in the parliamentary debate on the code, noted that 'The Government will support the code by providing the Information Commissioner with a list of minimum standards to be taken into account when designing it.' See column 1440 of Hansard, available here: https://hansard.parliament.uk/lords/2017-12-11/debates/154E7186-2803-46F1-BE15-36387D09B1C3/DataProtectionBill(HL)

- To provide a greater level of specificity about what the Commissioner expects online services used by children to do in order to comply with the GDPR, the DPA 2018 and PECR.

2.4 Approach to the code

When devising the code the Commissioner consulted a wide range of stakeholders including industry bodies, child advocacy groups and civil society organisations and, importantly, children and parents themselves. An initial call for views helped to shape the overall direction, together with a list of areas provided by Government. A full public consultation was undertaken on the draft Code and the final version reflected significant changes to clarify a range of areas, including age assurance. Assurances were also added to the face of the code to emphasise the Commissioner's commitment to taking a risk based and proportionate approach to its requirements and assessing conformance with the standards.

The code does not constitute new law, rather it sets out high-level standards that organisations offering information society services likely to be accessed by children should meet. The standards and associated guidance explain how relevant organisations should apply the existing requirements in the GDPR, the DPA 2018 and PECR when developing their services in order to recognise and cater for child users.

The code takes a privacy by design approach, consistent with other regulatory approaches such as the recent government consultation *Secure by design*[20] in relation to cyber security and the development of standardised approaches to ensuring website accessibility which are now reflected in W3C standards. While work will be required to ensure existing services conform to the code, it will provide an easy reference for organisations seeking guidance on the areas they must consider to ensure their services comply with the legislation and ensure that new services will have these considerations built in from the start, making the process both more efficient and more effective.

2.5 Scope of the code

The code applies to ISS that process personal data and are likely to be accessed by children in the UK. An ISS has the same meaning as within the GDPR and is defined as any service normally provided for

[20] https://www.gov.uk/government/collections/secure-by-design

remuneration, at a distance, by electronic means and at the individual request of a recipient of services. This is a broad definition which means that most online services are information society services including apps, programmes and many 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.

Services that are not deemed 'relevant ISS' and are outside the scope of the 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. Traditional voice telephony and general broadcast services, such as scheduled television and radio transmissions aired to a general audience are not relevant ISS, though if a service offers general broadcast and an on demand service then the latter will be covered by the code. Finally, the code does not apply to websites or apps offering online counselling or preventive services to children.

2.6 Affected groups

Accordingly, the key affected groups are:

Child data subjects in the UK whose personal data is processed by the ISS that they are likely to access. A data subject is an individual who is the subject of personal data, and for the purposes of the code, a child is any individual between the age of 0 and 17. Child data subjects will be directly affected by the code as it will govern the way in which their personal data is used. ONS data show a total of 14.2m dependent children in all types of family in the UK in 2019.[21]

Parents (or those with parental authority) of child data subjects using ISS may be affected by the code as it may alter the level and nature of their parental intervention. ONS data show 29.8m people in all

[21] See Table 2 of the ONS Families and Households dataset, https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/datasets/familiesandhouseholdsfamiliesandhouseholds.

types of family with dependent children in the UK in 2019, suggesting that there are up to 15.6m parents or those with parental responsibility.[22]

Providers of relevant information society services, meaning ISS that process personal data and are likely to be accessed by children in the UK. The number of these providers is discussed in further detail below.

Providers of other services, for example providers of third party safety technology or age assurance solutions may be affected by the code as it may positively impact demand for their services. According to the Government's recent report, *Safer technology, safer users*, the UK is a world leader in Safety Tech, with 70 dedicated Safety Tech businesses.[23] All but one of these are micro companies or SMEs, and the sector has grown rapidly with an estimated 35% annual growth rate since 2016. In 2019 the annual revenue for the sector was £226 million. Government estimates are that these revenues could grow to £1bn in the UK by the mid-2020s assuming a comparable or higher growth trajectory in future years. Estimates are that the UK already represents 25% of international market share for independent Safety Tech providers.

The Commissioner, the data protection regulator, with primary responsibility for regulating the GDPR, and the DPA 2018. This includes investigating potential infringements of the underpinning legislation and using relevant enforcement powers as appropriate. The Commissioner will be affected as her office will need to provide advice, promote good practice and assess conformance to the code.

The justice system will be affected as, in accordance with s127(3) of the DPA 2018, a court or tribunal must take into the provisions of the code in any proceedings before it to the extent that it appears relevant to the questions it is required to determine.

Wider society, which may be affected by the code as it may change the way in which online services are offered to both children and other users and may bring about wider societal change.

[22] See Table 4 of the ONS Families and Households dataset, https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/datasets/familiesandhouseholdsfamiliesandhouseholds.
[23] Safer technology, safer users, https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech.

2.7 Principles and approach

This section explains the approach that the Commissioner has taken to producing this impact assessment, which aims to identify, as far as possible, the impacts of the code and whether the proposals deliver a positive impact to society. It explains the counterfactual, which is the baseline for the analysis, and the analytical framework and principles that she has applied in identifying costs and benefits.

2.7.1 The counterfactual

The counterfactual in an impact assessment is the baseline against which the incremental impacts of the introduction of a policy can be estimated. As explained above, the code has some incremental impacts but the requirement to produce it and some of the standards are not incremental but rather stem from s123 DPA 2018 and the GDPR. Accordingly, the Commissioner assumes that absent the introduction of the code the data protection legislative framework would continue in its present form.

In applying this counterfactual the Commissioner assumes that the number of businesses and other organisations processing personal data would remain unchanged going forwards, and also that the number of data breaches would remain unchanged. These assumptions are subject to uncertainty and the Commissioner notes that to the extent that more firms would be affected in future and greater levels of harm might be experienced in the counterfactual this assessment will understate the impacts.

2.7.2 Analytical approach

In order to identify and assess, as far as is possible, the impacts of the code on society the Commissioner's approach is to address each of the standards in turn, consider its impacts and assess whether or not it is an incremental impact of the code. The impacts of the code therefore fall under three broad headings:

- The **incremental impacts of the code** – these are the impacts that the Commissioner considers can be attributed directly to the code. Where the Commissioner has provided a level of specificity in how she expects ISS providers to comply with the GDPR, that is neither an existing explicit requirement of the legislation, nor a direct or inevitable consequence of the wording of s123 DPA 2018, then she considers the impact to be truly incremental.

- The impact of **the scope and requirements of s123 DPA 2018** – the Commissioner considers that any requirements within the code that arise as a direct consequence of the wording and requirements of s123 DPA 2018 are not incremental impacts of the code. This is an important distinction because the Commissioner has no discretion to disregard, alter or otherwise address the impact of s123; this would require a change to the DPA 2018. The Commissioner has, however, included an assessment of these impacts within this document. This is because she appreciates that services within the scope of the code are unlikely to draw a distinction between the impact of s123 DPA 2018 and the impact of the code itself over and above this. She also notes that the impact assessment for the Data Protection Bill made no detailed assessment of the impact of the chosen wording of s123.
- The impact of **existing explicit requirements of the GDPR** – these are considered neutral in terms of the code. This is because ISS providers within scope should already be compliant with these explicit GDPR requirements and therefore should incur no additional or incremental costs in meeting the expectations of the code. Any benefits arising from such requirements are similarly benefits that can be attributed to the GDPR, so there is no incremental cost benefit from them also being included in the code.

Annex A contains a visual representation of the derivation of the different impacts of each standard in the code.

The assessment is focussed on the incremental impacts of the code, with attention to impacts affecting SMEs. Impacts are assessed using cost benefit analysis, which aims to identify the full range of impacts of the code, including effects on all of the affected groups identified above, and all types of impact, including indirect as well as direct impacts. However, it is important to bear in mind that it is not practical to undertake a forensic analysis of all the implications of the code.

The evidence base primarily constitutes desk-based research, responses to the call for evidence and consultation on the code, and previous analysis of related issues.

This assessment does not consider alternative options to drafting a statutory Code of Practice for the reasons set out above. It is simply an evaluation of the introduction of the code against the counterfactual. It is intended to assist Parliamentarians as the code is scrutinised and will

inform the Commissioner's development of the implementation support package.

2.7.3 Quantification

The nature of the code makes quantified analysis of the costs and benefits particularly challenging.

For example, in terms of the potential for costs falling on ISS providers within scope, the code leaves room for interpretation, with costs varying even between SMEs.

In addition, calculating the incremental costs of the code on the affected businesses is complex, as the nature of these costs will vary considerably depending on the sophistication and maturity of the businesses existing data protection systems and processes, the nature of the services they provide, the data processing associated with those services and the level of risk to children that processing poses.

Equally, on the benefits side, the nature of many of the benefits, such as reducing children's exposure to a range of online harms, increased trust in use of online services or increased control of children over their information, is challenging to quantify.

The analysis in this assessment has therefore focussed primarily on non-monetised impacts, supporting these with evidence including quantitative evidence where this has been possible. However, we will continue to engage closely with ISS providers during the implementation period to understand the costs in more detail, and ensure the package of support provided is targeted appropriately.

2.8 Regulatory constraints

The Commissioner has drafted the code within the following regulatory constraints:

- her remit, powers and duties as set out in the GDPR and the DPA 2018.
- the obligations placed upon her by s123 of the DPA 2018.

She has also sought to take account of the intentions of Parliament and Government in providing her with a list of areas that she should consider addressing in the code.

3. Cost benefit analysis

We have looked in turn at the costs and benefits of the overall scope of the code, and of each of the 15 standards. As noted above, the analysis of these costs and benefits is, unless stated otherwise, qualitative.

The standards within the code are related and interdependent so there may be some overlap in the cost benefit analysis of the different impacts. This may be particularly the case for the wider benefits to children and society that arise from the code.

The Commissioner finds that there is a distinct incremental impact arising entirely, or in part, from a number of standards within the code. These impacts are set out in detail in section three. The extent to which these impacts will apply will vary depending on the data being processed.

Incremental impacts are those that the Commissioner considers can be attributed directly to the code because they provide a greater level of specificity about how organisations should comply with the GDPR where an existing explicit requirement does not exist and the obligation is not an inevitable consequence of s.123 of the DPA 2018.

The impacts attributable to existing legislative requirements are considered to be part of the counterfactual to this impact assessment (the baseline against which the impact of the code is measured), which the Commissioner has no discretion to amend. This includes two impacts raised by stakeholders as being of most concern: the impact on existing business models of not being able to process children's personal data for the purposes of behavioural advertising by default, and the cost of providing different versions of services for users of different ages. The Commissioner considers these arise from GDPR, PECR and s123 of the DPA 2018.

We have also identified an additional familiarisation cost of £206 for each provider of ISS, which represents the time and resource required to familiarise themselves with the requirements of the code. On the basis that the code will impact on around 290,000 business, this results in a one-off familiarisation cost of £60m, or around £2 for each of the children and parents (or those with parental responsibility) noted above. This cost is attributable to the s123 requirement to the Commissioner to produce a code. As part of developing the code the Commissioner sought to ensure maximum clarity and readability while still providing the necessary information.

The Commissioner has committed to providing a significant package of advice, guidance and support to assist providers of ISS within the scope of the code in conforming with these requirements. This will be informed by further stakeholder engagement and will give particular focus to support small and medium organisations that have more limited resources to address the code's requirements.

3.1 The scope of the code

3.1.1 The issue/problem to be addressed

Harms to children that arise from the use of their personal data online can arise from any service they use, not just those that are specifically designed for or targeted at children. Similarly, the potential for harm to arise from data processing depends upon the way that data is used by individual services (which can vary greatly) rather than on the size of business or the type of service it provides.

3.1.2 Policy objective

The scope of the code was set by Parliament in s123 of the DPA 2018. It includes ISS 'likely to be accessed by children' rather than just those designed for, or targeted at, children. Small and micro businesses were not excluded. This reflects the intention of Parliament to ensure that all services that children use in practice were covered, in order to minimise harms that they may suffer arising from the use of their personal data.

The Commissioner's policy objective in drafting the code was to ensure the scope and coverage intended by Parliament was implemented, whilst also allowing services to take a proportionate approach to conformance, taking account of the nature of their data processing and the potential harms to children that arise from that processing. The Commissioner does not have discretion to change the scope of the code or to disregard the intention of Parliament in this respect.

3.1.3 Scale of coverage

The choice by Parliament to set the scope of the code as it did means that the number of services affected by it is likely to be very significant, covering a majority of online services. The impact assessment undertaken

for the DPA 2018 does not include any estimate of the number of services likely to be impacted by the scope of s123, nor of Article 8.[24]

While national statistics on the number of businesses in the UK are available from the Business Population Estimates (BPE)[25], the way in which businesses are categorised does not readily map onto the scope of the code. For example, in estimating the number of providers of 'Information Society Services', data are available for the 'Information and Communication' industry, as well as the narrower 'Information Service activities' division. However, both of these will omit businesses covered by the regulation, such as retail businesses with an online presence, and in the case of the former will also include communications businesses which are explicitly excluded from ISS.

As an alternative source, DCMS, in its response to the Online Harms White Paper in early 2020 estimated that 'fewer than 5% of UK businesses will be in scope of this regulatory framework'.[26] Based on the BPE estimate of 5.9m businesses in the UK in 2019 this would suggest an upper bound of around 290,000 businesses affected.

This DCMS estimate measures organisations with an online presence, focussing on user-generated content and peer-to-peer interaction. While this definition is narrower than that of ISS, it is also the case that not all of these businesses will provide services 'likely to be accessed by children'. While we anticipate there could be a wider set of ISS in scope of the code than are captured in the estimate for online harms, it is not certain which of these effects will dominate the other, and in the absence of further evidence we have adopted the estimate of 290,000 providers of relevant ISS.

3.1.4 Cost to providers of ISS

The scope of the code is likely to give rise to one-off familiarisation costs to providers of ISS, in order for them to read and familiarise themselves with the content.

As part of developing the code the Commissioner sought to ensure maximum clarity and readability while still providing the necessary information. The code contains 34,402 words and has a Fleisch reading

[24] Where an information society service is offered directly to children and their data is processed on the basis of consent, Article 8 of the GDPR states that the processing will only be lawful to the extent that the consent is given or authorised by the holder of parental responsibility over the child. In the UK this requirement applies where the user is under 13.
[25] See https://www.gov.uk/government/statistics/business-population-estimates-2019.
[26] See https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response.

ease score of 44.2. Assuming a reading speed of 75 words per minute this suggests a reading time of 7.64 hours.

This can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings (ASHE).[27] Assuming that the relevant 'occupational group' is 'Managers, Directors and Senior Officials', the 2019 median hourly earnings (excluding overtime) for this group is £22.07. This hourly cost is uprated for non-wage costs using the latest figures from Eurostat and in line with Regulatory Policy Committee guidance,[28] resulting in an uplift of 22% and an hourly cost of £26.91.

The reading time and hourly cost lead to a familiarisation cost of £206 for each provider of ISS, which on the basis of around 290,000 business results in a one-off familiarisation cost of £60m. On the basis of there being 14.2m dependent children in all types of family in the UK in 2019 and up to 15.6m parents or those with parental responsibility, this implies a cost of around £2 for each of these individuals.

In some case the costs to providers of ISS may be lower, for example if they are quickly able to ascertain that the code does not apply to them. However, there may be other familiarisation costs to businesses, such as costs of dissemination and training. Where the issues are more complex, legal advice (with resulting costs) may also be needed. In some cases it is also possible that market research might be needed or other evidence of user behaviour, for example to test whether their service is 'likely to be accessed' by a child by researching similar services and testing access restriction measures.

SMEs in particular are less likely to be able to rely upon in-house expertise in these cases and so may need to buy in third-party advice.[29] However, this is uncertain in all cases and it would be very difficult to estimate the extent of the change, numbers of businesses affected, or to separate the specific costs out from those that would be incurred in any case. It is therefore not possible to estimate these costs.

[27] See https://ec.europa.eu/eurostat/statistics-explained/index.php/Hourly_labour_costs and https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/bulletins/annualsurveyofhoursandearnings/2019.

[28] See guidance in https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs__August_2019.pdf.

[29] Articles 37(2) and (3) of the GDPR enable businesses to appoint a joint DPO, which may allow organisations to share costs. However, we do not have figures on the extent to which this has been adopted.

3.1.5 Wider costs

In terms of other affected groups, there will be a cost to the ICO of providing appropriate advice and support to providers of ISS in relation to questions of whether their services are within scope, and, in the event of an investigation, considering whether an online service has correctly assessed whether it is in scope or not.

We anticipate this advice and support forming part of the package of support to be provided by the ICO, however given uncertainty about the number of providers of ISS who would seek this advice, and the context-dependent nature of the work involved it has not been possible to estimate these costs.

3.1.6 Benefits to providers of ISS

A potential benefit of the need for online services to establish whether they are an ISS or not is that it is consistent with, and should therefore help them to comply with, other statutory requirements, specifically Article 8 GDPR and the eCommerce Regulations 2002.

Any additional understanding that services have of their user base, including via market research when appropriate, is likely to lead to businesses offering existing and in some cases new services that better meet the needs of their users.

3.1.7 Wider benefits

The broad coverage of the code as mandated by Parliament means that children will be less likely to be exposed to the harms outlined above. In addition, parents would be reassured that the services that their children are likely to access will feature high privacy by default safeguards to better protect them against social and commercial harms. Our research found that parents want their children to be able to use services but are also overwhelmed by the amount of privacy information available when seeking to protect their children.[30]

Increased parental confidence can in turn be expected to contribute to greater trust in ISS and associated positive use of online services by children. Reducing the potential for harms and improving outcomes for children should have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and

[30]Towards a better digital future, ICO / Revealing Reality 2019, P.13. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf

emotional wellbeing and in raising future generations of well-balanced, emotionally resilient adults.

The increased clarity on scope that the code provides will also yield benefits to the ICO when investigating potential infringements, and to the justice system.

3.1.8 Categorisation of impact

The Commissioner considers that the impact of **the broad scope of the code** is a direct and inevitable consequence and therefore **an impact of s123 of the DPA 2018.**

The Commissioner considers **the impact of establishing whether a service is an ISS** or not to be largely **neutral** in terms of the code.

This is because services already need to know if they are an ISS in order to consider and, if necessary, comply with the requirements such as the e-Commerce directive.

Further, services which rely upon consent as their lawful basis for processing under the GDPR and offer their service directly to children also already need to know if they are an ISS in order to consider, and if necessary comply with, the existing requirements of Article 8 of the GDPR.

Even if the above were not the case, the Commissioner would consider the impact of establishing whether a service is an ISS or not to be an inevitable consequence of the chosen wording of Parliament of s123 DPA 2018 which imports the existing definition. As the Commissioner has no discretion to disregard this wording she considers that any costs arising from the need to answer this question would be an impact of s123 DPA 2018, rather than a direct impact of the code.

The Commissioner considers **the impact of establishing whether a service is 'likely to be accessed by children'** to be an inevitable consequence of the chosen wording of Parliament of s123 DPA 2018. As the Commissioner has no discretion to disregard this wording she considers that any costs arising from the need to answer this question would be **an impact of s123 DPA 2018**, rather than a direct impact of the code.

The Commissioner considers that **the familiarisation cost associated with the code**, calculated as a one-off familiarisation cost of £60m, is an

impact of the s123 DPA 2018 requirement to the Commissioner to produce a code.

3.1.9 Other options considered but not taken forward

As the scope of the code has been set by Parliament in S123 DPA 2018 the Commissioner had no discretion to consider alternative scope options.

3.2 Standard 1 – the need to consider the best interests of children

3.2.1 The issue/problem to be addressed

Whilst some ISS specifically consider the needs of children in their design, many currently do not. This means that children are accessing services that do not take account of their age, or their limited capacity to understand and control the consequences of how their personal data is used. This allows services to be designed in a way that potentially puts commercial interests above the best interests of children.

3.2.2 Policy objective

S123 DPA 2018 requires the Commissioner, in preparing the code, to have regard to the UK's obligations under the United Nations Convention on the Rights of the Child (UNCRC), which includes consideration of the best interests of the child. It also requires the Commissioner to prepare guidance on standards of age appropriate design which appear to her to be desirable, 'having regard to the best interests of children'.

This reflects the intention of Parliament, as expressed by Baroness Kidron during the debate to the Data Protection Bill, that the standards within the code should 'clarify the expectation on services to design data practices that put the "best interests" of the child above any other consideration, including their own commercial interest.'

The Commissioner's policy objective in drafting the code was to ensure the above intentions of Parliament were implemented, whilst also allowing services to take a proportionate approach to conformance, taking account of the nature of their data processing and the potential harms to children that arise from it.

The Commissioner also intended to bring about a change in the way services account for the needs of children in their design. By introducing an explicit need to consider the best interests of children, the

Commissioner sought to put the needs of children front and central in the design process and to trigger services to think about the wider consequences or impacts of their processing. Her ultimate objective is for this to lead to a reduction in the potential for harms to children arising from data processing.

3.2.3 Costs to providers of ISS

For services that are already child-centric or designed with the welfare of children in mind this should require little, if any, change to existing processes and considerations. It should also not result in significant changes to end products or costs for providers of in-scope online services.

For services used by children but not already designed with the welfare of children in mind this may require significant changes to the processes by which services are designed and developed, which are likely to incur costs.

In the most significant cases where children's data is central to the service, and risks are high this may also mean that some revenue streams are lost and/or end products are not as profitable, so the overall cost of this requirement to some services may be significant. However, given the available information it has not been possible to quantify this. The Commissioner will consider whether it is feasible to gather evidence on this at a later stage, potentially at the review in 2022.

3.2.4 Wider costs

There may be a wider cost to adult users if they have to go to additional effort to access elements of service that are suitable for them but not children as a result of protections for young people that are built in.

There will also be a cost to the ICO in providing appropriate support and advice and, in the event of an investigation, assessing conformance to this standard.

3.2.5 Benefits to providers of ISS

Considering the best interests of children as part of the design of services should improve services and make them more desirable to users. It should also enhance the reputation of compliant providers, and more generally increase the trust and use of ISS, to their benefit.

Many online services already recognise the value of designing in safeguards, for instance to allow users to report harmful content, and children are using these services. For instance, according to Ofcom's

Online Nation report a third of 12-15-year olds (29%) say they have acted to report harmful content that they have seen online and 15% had reported content to a site.[31] Organisations that have already invested in thought and action to embed these kind of child-centric approaches will be supported by regulation that creates a more level playing field for organisations wishing to implement this approach.

3.2.6 Wider benefits

Making consideration of the best interests of children a requirement of the code should improve outcomes for children and reduce the potential for harms arising from processing (as set out in section 2.1 'Problem under consideration' above.)

Reducing the potential for harms and improving outcomes for children should have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.2.7 Categorisation of impact

The Commissioner considers the impact of **considering the best interests of children** in the design of service to be an inevitable consequence of the chosen wording of Parliament of s123 DPA 2018. As the Commissioner has no discretion to disregard this wording she considers that any costs arising from the standard to be **an impact of s123 DPA 2018**, rather than an incremental impact of the code.

3.2.8 Other options considered but not taken forward

The Commissioner considered that for her to identify and list within the Code what would be in the best interests of children in the context and nuance of the many and varied services that it covers would be impracticable, inflexible, and would run contrary to the principles of the GDPR that allow and require data controllers to assess their own processing risks in a proportionate manner and demonstrate their accountability for their decisions and practices.

[31] Online Nation 2020 Report, Ofcom, P.31.
https://www.ofcom.org.uk/__data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf

3.3 Standard 2 –the need to undertake a data protection impact assessment (DPIA)

3.3.1 The issue/problem to be addressed

Where services don't use a framework to consider risks arising from processing and the wider consequences of their data use, then the potential for risks to remain unidentified and harms to arise is increased.

3.3.2 Policy objective

To ensure that ISS providers properly assess the impact of their data use on children and mitigate any risks to the rights and freedoms of children that arise from that processing.

3.3.3 Costs to providers of ISS

The GDPR requires organisations to do a DPIA before they begin any type of processing that is likely to result in a high risk to the rights and freedoms of individuals. This is not about whether a service is actually high risk, but about screening for potential indicators of high risk.

The ICO is required by Article 35(4) of the GDPR to publish a list of processing operations that require a DPIA. This list supplements GDPR criteria and relevant European guidelines, and includes: "the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children." DPIAs are also required for online services that include (but are not limited to): innovative technology; large-scale profiling; biometric data; online tracking; matching or combining of datasets from different sources; and processing data that might endanger the individual's physical health or safety in the event of a security breach.[32]

We believe that the majority of ISS in scope of the code are therefore likely to already need to conduct DPIAs. For these businesses there will need to be some extra consideration of how they meet the standards in the code, which will bring some incremental costs, but should not require much change to existing data accountability processes.

A small number of ISS may be providing services that are not offered directly to children but are likely to be accessed by them and which do

[32] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

not include any of the other data processing activities set out above that would require them to do a DPIA. These services will need to incorporate this into their existing processes, which is likely to lead to additional costs. However, given the lack of any other data processing factors that would trigger a DPIA, completing these should be relatively straightforward.

We would expect larger ISS providers (such as the large tech companies) to already employ the services of a Data Protection Officer (DPO) who should be familiar with DPIA processes and able to advise. SMEs (depending on the nature of the service they offer) may be less likely to have this expertise already available and may have to buy it in, so the costs of undertaking a DPIA may be proportionally higher for them.

These costs will in part be mitigated by provision of ICO resources, such as example DPIAs and advice and support in the questions to ask and the factors to consider, during the transition period.

We have considered whether it is possible to quantify the costs of incremental DPIAs. However, the costs of completing a DPIA are uncertain, the extent to which work is required (ranging from a need to check existing DPIAs to make sure they take account of the standards to a need to complete a new DPIA) is specific to the context of each business, the services they offer, their risk appetites, existing DPIA provision and the application of the ICO's mitigations. As a result, we have been unable to estimate these costs.

3.3.4 Wider costs

There will be a cost to the ICO for providing a formal response to any DPIAs submitted for prior consultation. In the Impact Assessment for the Law Enforcement Directive the costs of a DPIA authorisation were estimated at between £200 and £400.[33]

There will also be costs to the ICO in providing appropriate support and advice and, in the event of an investigation, assessing conformance to this standard. However, given the uncertainty around the number of incremental DPIAs that might arise, and the context-dependent nature of the work that would be required it has not been possible to quantify these costs.

[33] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711221/Law_Enforcement_Directive_Impact_Assessment.pdf.

3.3.5 Benefits to providers of ISS

Using a DPIA process should help online services within scope to identify and mitigate risks arising from their data processing at an early stage, saving the costs involved in redesigning services later down the line, or 'bolting on' amendments to a service. Whilst for some services there may be a cost to altering existing services, taking a by-design approach from the beginning should become routine and over time reduce the costs of resolving problems later. Over time embedding these design principles should ensure that they are a routine consideration for everyone involved in product development, whether from commercial, legal or design teams and there should be an efficiency saving as it becomes more familiar. Examples of this approach working to good effect include the development of standardised approaches to ensuring website accessibility which are now reflected in W3C standards and also in implementing security by design in relation to cybersecurity[34].

Organisations can also use the DPIA to demonstrate their accountability and how they addressed each of the standards including in the event of a complaint and regulatory investigation by the ICO. It is also likely to assist in the event of legal action in the courts because organisations will have evidence to support their case in court.

3.3.6 Wider benefits

Completing a DPIA should mean identification of consequences of processing and potential for harm, allowing mitigation measures to be put in place and leading to a reduction in harms to children. Reducing the potential for harms and improving outcomes for children should have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

In terms of other affected parties there would be benefits to the ICO in the case of an investigation if the business had a readily available and good quality DPIA addressing all the relevant standards in the code to demonstrate its accountability.

3.3.7 Categorisation of impact

The GDPR already requires a DPIA for any processing that, 'is likely to result in a high risk to the rights and freedoms of individuals'. It requires

[34] https://www.gov.uk/government/collections/secure-by-design

the ICO to publish a list of processing operations that need a DPIA. This list includes 'the use of the personal data of children or other vulnerable individuals for marketing purposes or other automated decision-making, or if you intend to offer online services directly to children', in addition to a range of other areas where a DPIA would be necessary. This means that many services within the scope of the code should already be conducting a DPIA. The Commissioner therefore considers the impact of the **DPIA standard** to be **largely cost neutral** in terms of the code.

For a **minimal number of online services** that would not already be required to undertake a DPIA by the GDPR, the Commissioner considers that the cost of completing a DPIA would be an **incremental impact** that arises directly from the code.

The **obligation to consider how services conform to the specific standards in the code** as part of the DPIA is a new requirement and therefore an **incremental impact** that arises directly from the code.

3.3.8 Other options considered but not taken forward

None.

3.4 Standard 3 – the need to establish the age of individual users with an appropriate level of certainty

3.4.1 The issue/problem to be addressed

Many online services are currently provided without consideration of the age of the user, or differentiation in how their personal data is used. This creates the potential for children's personal data to be used in ways that are not appropriate to their age and may lead to various harms (see section 2.1 'Problem under consideration', for further detail).

3.4.2 Policy objective

To prevent children's personal data being processed in ways that are inappropriate to their age or that lead to harm.

S123 of the DPA 2018 requires the Commissioner, in preparing the code, to account for the fact that children have different needs at different ages. The Commissioner considers that this means that ISS providers within scope will need to have an understanding of the age of its individual users. The intentions of Parliament in this respect are reflected in the

following comments made by Baroness Kidron in the debate to the Data Protection Bill, '[The amendments to the Bill] introduce a code that will set out the standards by which online services protect children's data. They set standards that are directly related to a child's age and the vulnerabilities associated with that age.'

The policy objective is to implement the intention of Parliament as expressed in s123 DPA 2018 whilst also allowing services to take a proportionate approach to conformance, taking account of the nature of their data processing and the potential harms to children that arise from it.

3.4.3 Costs to providers of ISS

This standard does not mandate age verification. It states that services need to either establish the age of individual users with a level of certainty appropriate to the risks that arise from its data processing, or apply the standards in the code to all users.

Where risks arising from processing are particularly low then self-declaration of age systems may suffice, which would be relatively low cost.

Where risks are higher, organisations need to have a higher level of certainty about age. Organisations that do not already have proportionate age assurance measures in place and decide not to take the option of applying the standards to all users may incur costs in developing or buying-in such measures. Small businesses in particular are unlikely to be able to develop systems in-house and are likely to be reliant on third-party providers.

As the current marketplace in age assurance solutions is relatively immature there may be a limited choice of solutions which may make them more expensive to buy in (due to supply/demand considerations)[35]. The Commissioner has clarified on the face of the code that she will take account of the technological solutions available in the marketplace when assessing conformance with the standards, particularly for small businesses which don't have the resources to develop their own solutions.

Given the uncertainty around the extent to which age assurance systems or changes to services would be required, which will depend on the

[35] Following consultation, the Code was amended to clarify that the Commissioner will take into account the range and nature of age assurance solutions available when considering any action.

context of the firm in question, it has not been possible to quantify these costs.

3.4.4 Wider costs

There may be a wider cost to all users of online services (adults and children) in that they may be subject to age assurance processes before they are able to access online services. This is likely to be primarily a cost in time or convenience, although there may be some cases where a financial cost could apply, eg if a company decides to use hard identifiers to determine age, as some age verification approaches might take a nominal payment (eg 1p) from a credit or debit card as part of the verification process. However, the Commissioner has stated on the face of the code that companies should avoid giving users no choice but to provide hard identifiers unless the risks inherent in processing really warrant such an approach. This is because some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate.

It also represents a trade-off, in that all users of a service employing these kinds of age assurance techniques may need to give up some data in the interests of increasing protections for children. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults. It will therefore be important that this is done in the most privacy-enhancing and data limited way.

There will be a cost to the ICO in providing appropriate advice and support and assessing the suitability of age assurance measures in the event of an investigation.

It is also possible that there could be competition impacts of this requirement, to the extent that larger firms are better able to absorb the costs than SMEs and hence gain a competitive advantage. However, there are also likely to be competition benefits in terms of safety technology, as noted further below.

3.4.5 Benefits to providers of ISS

Proportionate age assurance measures could be a selling point that makes their services more attractive to users and their parents, because by gaining a better understanding of the user they are able to make the experience age appropriate.

3.4.6 Wider benefits

Reducing the potential for harms and improving outcomes for children should have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

This standard may lead to benefits for providers of safety technology services, and may be a driver of investment and economic growth in the UK safety tech industry as new age assurance solutions are developed. Government estimates are that UK safety technology revenues could grow to £1bn in the UK by the mid-2020s, assuming a comparable or higher growth trajectory in future years. Estimates are that the UK already represents 25% of international market share for independent Safety Tech providers.[36] This could lead to benefits to society from competition and a range of age varication/assurance services which are likely to be relevant in future online harms regulation and imminent video sharing platform regulations under Ofcom's remit. It would also benefit the UK by positioning us as a leader in this field and being able to export this technology as others regulate and need to buy it.

3.4.7 Categorisation of impact

Services which use consent as their lawful basis for processing are already required by Article 8 GDPR to get parental consent for any UK users under the age of 13. This means that there is an existing need under the GDPR to establish age (so services know whether parental consent is required) for any consent-based processing. So, for **online services which rely upon consent** this impact is considered to be **neutral** in terms of the code.

For **online services which don't rely upon consent** as their lawful basis for processing the Commissioner considers that requiring services to understand the age of individual users is an inevitable consequence of the wording of s123. The Commissioner has sought to mitigate this impact by allowing services an alternative of applying the standards in the code to all their users and by allowing a proportionate approach which takes account of the risks to children that arise from the data processing, but in

[36] *Safer technology, safer users: The UK as a world leader in safety tech,* DCMS / Perspective Economics 2020, P9.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf

any case considers that this is **an impact of s123** rather than a purely incremental impact of the code.

3.4.8 Other options which were considered but not taken forward

The consultation draft of the code took a more rigid approach to age assurance, requiring services to apply the standards to all users unless they had robust age verification measures in place. This was amended in response to consultation comments that this approach was not proportionate and did not take account of the fact that some processing poses less risk of harm to children than others.

3.5 Standard 4 – the need to provide age appropriate privacy and other information

3.5.1 The issue/problem to be addressed

Much information provided by online services is not provided in a way that is accessible to children and takes account of their age. This means that many children do not understand how their personal data is used by online services and what the consequences of that use might be. This can lead to their commercial exploitation and infringement of their privacy rights.

3.5.2 Policy objective

S123 of the DPA 2018 requires the Commissioner, in preparing the code, to account for the fact that children have different needs at different ages.

The Commissioner's policy objective is to increase the accessibility of information provided to children using online services to help them better understand the consequences of how their data is used and to reduce exploitation due to their lack of understanding, whilst also allowing a proportionate approach that takes account of the risks arising from the data processing.

3.5.3 Costs to providers of ISS

For services that already provide child friendly information this should not require much, if any, change.

For services that don't already provide child friendly information, development costs may be incurred.

Where it is not viable to provide a single, accessible to all, version of information then costs may be incurred in developing and providing different, age appropriate versions. Whether several versions are required will depend on the specific data risks arising from a particular service, the range of users and the degree to which the messages being given to those users vary. Where there are users within several age ranges and each require different messages/approaches the costs will be higher. Small business representatives in particular have indicated this may be a significant cost, but we do not have sufficient evidence to quantify these costs.

3.5.4 Wider costs

In terms of other affected parties there will a cost to the ICO in providing appropriate support and advice and assessing whether this standard has been conformed to in the event of an investigation. However, the uncertainty and context-specific nature of this work means that it is not possible to estimate this impact.

3.5.5 Benefits to providers of ISS

Providing clearer and more accessible explanations of their services may make these more attractive to users, improve the overall user experience and build greater trust and loyalty. It may also be a differentiating factor used by services to compete and gain new users. It could also mitigate the risk of complaints from users who feel they have been treated unfairly.

3.5.6 Wider benefits

There is a benefit to children in educating them about how their personal data is used so they are better placed to exercise informed control over their online information and they feel that they are treated fairly. Children often express frustration at the length of privacy notices and terms and conditions that don't mean a great deal to them. They are likely to have an improved user experience.

There is a benefit to parents in gaining a better understanding of what is happening to their children's data so that they can support their children and intervene where necessary from a more informed standpoint, whilst feeling reassured that their children are developing greater awareness and resilience from this age appropriate information.

There may also be a wider benefit to adults who similarly do not understand how their personal data is being used and the potential consequences of that use.

Ensuring users receive age appropriate explanations about what is happening with their data and why will help to ensure they feel fairly treated. In the longer term this may reduce the number of complaints to services and to the ICO.

3.5.7 Categorisation of impact

Article 12 GDPR already requires ISS providers to 'use clear and plain language, in particular for any information addressed specifically to a child.' It does not, however, explicitly require the language used to be suited to the age of the individual child. However, s123 of the DPA 2018 requires the Commissioner, in preparing the code, to have regard to the fact that children have different needs at different ages. This makes it clear that it is not sufficient to just consider the needs of children as one homogeneous group, which gives rise to **the potential need for different versions of information** or different messaging as a **direct impact of the wording of s123 DPA 2018.**

3.5.8 Other options considered but not taken forward

In response to consultation comments we amended the code to allow that there may be some circumstances under which it is proportionate to provide a single version of information that is accessible to all, whilst retaining the need to provide different versions where this is genuinely needed to meet the needs of children of different ages.

3.6 Standard 5 - the need to establish when use of data may have a detrimental effect on children and to design services so that data is not used in this way

3.6.1 The issue/problem to be addressed

The use of personal data by online services is wide and varied and often does not take account of the age of the user. This means that there is potential for data to be used in ways that are detrimental to the health and wellbeing of children. In particular personal data is often used to inform content feeds, or suggest content to users and sometimes this content is not age appropriate.

3.6.2 Policy objective

To reduce harms to children arising from inappropriate content feeds or other uses of personal data, whilst taking a proportionate approach to the level of expertise she expects online services to have in matters of children's health and wellbeing.

3.6.3 Costs to providers of ISS

Where providers do not already make efforts to follow relevant voluntary industry codes as a matter of good practice, costs may be incurred in identifying relevant industry codes of practice, other regulatory provisions or Government advice on detriment to children's wellbeing.

Costs may also be incurred in developing algorithms that cross reference other regulatory provisions and introduce processes such as 'content tagging' when using data to inform content feeds. The costs will be lower where services already implement such systems as a matter of good practice or to conform to existing industry standards or codes of practice.

3.6.4 Wider costs

There will be a cost to the ICO for providing appropriate support and advice and of assessing conformance to the code in the event of an investigation. If the ICO were to take forward the option of producing and maintaining a log of relevant advice there would also be a cost involved in this.

3.6.5 Benefits to providers of ISS

Designing services so as to avoid using data in ways that is detrimental to children will make services more attractive to users and could become a selling point. By preventing instances of harm as a result of processing of personal data organisations will also protect and potentially enhance their reputations, as well as avoiding potential regulatory action and any costs associated with this.

Cross referencing data use to wider existing regulatory requirements will ensure overall compliance is improved and increase services ability to demonstrate accountability.

3.6.6 Wider Benefits

Although children want to feel safe online, they are concerned about missing out on experiences that their friends and peers are having. In 2019 research by the ICO/Revealing Reality, many children felt that there

was a 'binary choice between maintaining privacy and keeping up with their peers.'[37] The report also found that children of all ages expressed concerns about who has access to their personal data and geolocation information. Younger children were especially concerned about being identified by strangers who may do them harm.[38]

Many children have directly experienced harms online, as is evidenced by the Ofcom Online Nation 2020 report. This research found that 26% of 12-15s said that in the past year they had come across bullying, abusive behaviour or threats online, 29% had encountered unwanted contact online, 24% trolling, 19% someone pretending to be someone else and 10% stalking or harassment. Nearly one in ten (9%) said they had come across content promoting self-harm.[39] Half of 12-15 year olds reported seeing hateful content online against particular groups of people, an increase of a third from 2016.[40]

Online harms disproportionately impact on vulnerable children already experiencing wider real-world issues. Research by Internet Matters found that "online, despite the advantages of technology, some children's vulnerabilities are exacerbated, and others are ill prepared for safe internet use."[41] Support systems for vulnerable children have not caught up with their needs for online protection: 58% of young carers and 48% of those in care had been cyberbullied compared to 25% of young people with no vulnerabilities. Meanwhile, 27% children with special educational needs (SEN) view sites promoting self-harm compared to 17% of non-vulnerable peers, and 25% often view pro-anorexia sites in contrast to 17% of peers.[42]

Reducing harms to children arising from inappropriate content feeds and other uses of personal data should improve outcomes for children and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

[37] Towards a better digital future, P9. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf
37 Towards a better digital future, P.16, https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf
[39] Online Nation 2020 Report, P.31. https://www.ofcom.org.uk/__data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf
[40] Media use and attitudes report, 2019, p.1. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf
[41] Vulnerable Children in a Digital World, Internet Matters 2018, P7. https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf
[42] Internet Matters 2018, PP22-23. https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Vulnerable-Children-in-a-Digital-World.pdf

Children will also have greater confidence to engage with services in the knowledge that they have been tailored to their needs to avoid them seeing content that they feel is upsetting or damaging as a result of the personalisation within the service. They will also have greater protection from feeling pressured to make in-game purchases. Currently we know children do feel this pressure: the *RipOff Games* report by Parent Zone found that 76% of children feel that online games try to make [them] spend as much money as possible.[43]

3.6.7 Categorisation of impact

Where **other regulatory provisions are compulsory**, rather than voluntary, then ensuring that personal data is not used contrary to such existing provisions is considered **impact neutral** in terms of the code (as the existing requirements should already prevent data being used in this way).

Where no other compulsory or statutory requirements apply, then though these obligations link back to underlying fairness requirements of Article 5(1) of the GDPR it is the AADC that makes them explicit obligations. The Commissioner therefore considered any such impact to be an **incremental impact of the code.**

3.6.8 Other options considered but not taken forward

The Commissioner has avoided expecting ISS providers to be or become experts in detriment to the health and wellbeing of children by allowing them to assess detriment by reference to other regulatory provisions and official advice.

The Commissioner considered not endorsing the Chief Medical Officer advice for online services to take a precautionary approach and remove addictive capabilities, given that the evidence on harm arising from strategies used to extend user engagement is disputed. However, she considered a precautionary approach was warranted because it had been recommended by professionals charged with protecting the health of UK children.

[43] The Rip off games. Parent Zone 2019, P.2. https://parentzone.org.uk/system/files/attachments/The%20Ripoff%20Games%20-%20Parent%20Zone%20report.pdf

3.7 Standard 6 – the need to uphold own published terms, policies and community standards

3.7.1 The issue/problem to be addressed

Many online services already set age limits for users and have rules in place that govern the service. However these are not always adequately upheld, which can lead to children accessing services that are not appropriate to their age group and consequently being exposed to harms arising from the processing of their personal data.

3.7.2 Policy objective

To ensure that when expectations have been set by a service as to how it operates, children and parents will be able to rely upon those expectations being met.

3.7.3 Costs to providers of ISS

For services which already uphold the rules they have set then no additional costs should be incurred.

Services who currently don't uphold their own rules may incur costs in doing so, however uncertainty and context-specific nature of this work means that it is not possible to estimate this impact.

3.7.4 Wider costs

There will be a cost to the ICO in providing appropriate support and advice and in considering whether or not a service has conformed to this standard in the event of an investigation.

It is also possible that there could be an indirect impact on competition because SMEs are less able to bear the costs than large providers, handing the latter a competitive advantage. However it has not been possible to estimate this.

3.7.5 Benefits to providers of relevant ISS

There are reputational benefits to services upholding their own rules. They are able to demonstrate that they provide the service and the conditions in which children's data is processed that they agreed to when the child signed up. This is likely to build user trust and confidence and potentially loyalty. This may also mitigate the risk of legal action being taken against services for breach of contract.

3.7.6 Wider benefits

This standard should lead to fairer treatment of all consumers in that they should receive the service that they have been led to expect.

This should reduce the potential for children to be exposed to harms by virtue of accessing services that haven't been designed for their age group. Reducing harms to children should improve outcomes for children and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.7.7 Categorisation of impact

Although this links back to underlying fairness requirements of 5(1) it is the code that makes this an explicit requirement. Therefore the Commissioner consider **the need to uphold a services own published terms** to be an **incremental impact of the code.**

3.7.8 Other options considered but not taken forward

The Commissioner considered restricting this standard to only cover terms and conditions related to the use of personal data. However, she considered that this would not address the issue of personal data being collected on the basis of expectations of service that are not upheld.

3.8 Standard 7 – the need to provide high privacy settings by default

3.8.1 The issue/problem to be addressed

Currently many online services configure their privacy settings in order to maximise the amount of data captured, using this data to fund underlying business models or product development.

Ofcom's Online Nation 2020 report outlined adult awareness of four common methods[44] for internet companies to collect personal information. While awareness of the use of cookies for data collection was high (78% in 2019), only 39% of adults were aware of all four methods. If it can be assumed that children would have the same, or likely lower,

[44] Four methods of collecting personal data sited in the Online Nation 2020 report were using cookies, collecting information from social media accounts, asking customers to register with a website or app, and using apps on smartphones to collect data.

awareness of how data is collected, this would mean that when children access services their data is often collected and used without them realising this is happening or understanding the implications.

Research by ICO/Revealing Realities found that although children were aware of the outcomes of profiling, such as recommended videos on YouTube, few understood the process of profiling and the mechanisms involved. This was attributed to the fact that children were less aware of data that platforms and websites collected indirectly, which was especially apparent in discussions about cookies.[45]

Ofcom research revealed a correlation between levels of online confidence and attitudes to use of personal data. For children between 12-15 years old, of those who described themselves as very confident online users, 44% were happy for ISS to use personal information to guide recommended content, and 40% accepted using data for targeted advertising. For users who were not confident, the corresponding figures fell to 28% and 30%.[46]

The Horizon Digital Economy Research Institute at the University of Nottingham noted in its 2018 response to the ICO's AADC consultation that children are less likely to engage privacy settings when experimenting with new apps. They tend to leave their personal data on default settings and tend not to fully close apps that they are no longer using.[47] This allows ISS to continue to track children's personal data even when they are no longer actively using apps or services.

The ICO/Revealing Realities research found that eight in 10 parents and carers felt that sharing data with third parties so that they can target their children with advertising should be switched off by default. Older children (13+ years old) favoured having privacy settings set as high by default for all their personal data, which they felt would give them more control.[48]

3.8.2 Policy objective

To ensure that children's personal data is protected by default, without them or their parents having to take any action. Ultimately the objective

[45] Towards a better digital future, pp28-29. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf
[46] Online Nation 2020 Report, p26-28. https://www.ofcom.org.uk/__data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf
[47] Horizon Digital Economy Research Institute response to AADC consultation, 2018. https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260169/horizon-digital-economy-research-insitute-university-of-nottingham.pdf
[48] Towards a better digital future, pp28-29. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf

is to reduce the potential for harms to children (see section 2.1 'Problem under consideration' for further detail) arising from their personal data being processed by default.

3.8.3 Costs to providers of ISS

Services that already provide high privacy settings by default should incur no additional costs.

Services that don't do this already may incur additional re-configuration costs. Where business models rely upon processing personal data by default (indications are that this is predominantly ISS funded by behavioural advertising by default) changing to high privacy by default is likely to lead to a reduction in revenue. Stakeholders have indicated that this is likely to be a highly significant cost that may render services no longer profitable/viable, but we have not currently seen any evidence that would allow us to estimate this impact.

While behavioural advertising appears to be the most common use of the process of maximising data collection through the use of privacy setting defaults, other instances could include where the ISS collects data on the use of one service which it then uses in the development of other services. In the former instance the changes could significantly reduce this revenue scheme as people are less likely to sign up to having their data shared in this way. In the latter instance, there could be some cost associated with updating systems to require children to opt in to have their data used in this way, and to informing them about this potential use, but we think this is likely to be a less significant cost than that posed by the inability to fund services using default settings that allow behavioural advertising.

3.8.4 Wider costs

There will be a cost in terms of additional effort or process for users who don't want to have high privacy settings and will need to change the default settings to make them lower privacy (reversing the status quo for many services where it is users who don't wish their data to be processed by default who incur the effort of making changes).

3.8.5 Benefits to providers of relevant ISS

Providing a child-friendly service by default should make services more attractive to users, become a selling point and prevent reputational damage to providers.

3.8.6 Wider benefits

There will be a benefit in reduction of process or effort for users who currently change low privacy default settings to make them high privacy or who would prefer these settings but do not have the skills, confidence, time or knowledge to make the changes. Previous research has shown that computer users rarely change their settings[49], and that for many of the largest social media sites, changing settings to high privacy involves more effort (click throughs) than retaining low privacy settings.[50]

This standard will reduce the harms (see section 2.1 'Problem under consideration' for more detail). Reducing harms to children should improve outcomes for them and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.8.7 Categorisation of impact

The opinion of the European Data Protection Board on the interaction between PECR and GDPR requirements confirms that the only appropriate basis for processing in the context of behavioural advertising is consent. As consent cannot, by definition, be provided by default, the impact on businesses of adopting a '**behavioural advertising off by default'** model is considered to be an existing impact of the GDPR and therefore **neutral** for the code.

For ISS that are using default settings that are not reliant on consent to collect data for other purposes such as **product development,** although this standard is linked back to the fairness principle at Article 5(1) of the GDPR it is the code which makes this an explicit obligation. The Commissioner therefore considers this to be an **incremental impact of the code.**

3.8.8 Other options considered but not taken forward

None.

[49]ttps://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/ (Do users change their settings?)

[50] Deceived by design, p17. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

3.9 Standard 8 - the need to minimise the collection and retention of personal data

3.9.1 The issue/problem to be addressed

Some online services collect personal data in case of future need or bundle elements of service together so that users cannot access one element without providing personal data needed for another. This can lead to children's personal data being collected unnecessarily.

3.9.2 Policy objective

To allow children a real choice over which elements of service they wish to use and therefore what personal data they need to provide.

3.9.3 Costs to ISS

Services that already limit personal data use to that which is necessary and proportionate to provide the elements of service being used should incur no additional costs.

Services that collect personal data beyond what is needed to provide the elements of service being used, or which 'bundle' elements of services together in 'all or nothing' packages may incur costs in re-designing services to separate out elements of service and provide consumer choice.

If services are reliant upon collection of more data than is necessary or bundling of services to fund business models then they may see a drop in revenue. However, given uncertainty and the content-specific nature of these costs it has not been possible to estimate them.

3.9.4 Wider costs

There will be a cost to the ICO in providing support and advice and assessing conformance to this standard in the event of an investigation, but for the reasons set out above it is not possible to estimate them.

3.9.5 Benefits to providers of ISS

Ensuring that data is minimised will reduce the risks that might arise from personal data breaches, thus also reducing the potential costs to providers as a result of penalties and legal action. It should also make services more attractive to users, become a selling point and prevent reputational damage to providers.

3.9.6 Wider benefits

This will reduce the potential for commercial exploitation of children and their exposure to privacy harms.

3.9.7 Categorisation of impact

Article 5 GDPR contains an explicit data minimisation provision which state that 'personal data shall be limited to what is necessary for the purposes for which they are processed'. We therefore consider the **need to minimise the collection and retention of personal** to be **impact neutral** in terms of the code.

3.9.8 Other options considered but not taken forward

None.

3.10 Standard 9 – the need to only share children's personal data if there is a compelling reason to do so

3.10.1 The issue/problem to be addressed

Sharing children's personal data with third parties can expose children to risks that go beyond those inherent in the original processing. Children may not know that their data is being shared or understand what the consequences of the data sharing may be. Where a child provides data which is then sold on for marketing or other purposes, the child may not understand that a commercial transaction is taking place, and even where they understand the trade-off between providing data as 'payment' for a free service, they may not have the tools to effectively judge the value of their data in this context.

A Norwegian Consumer Council Report found that "information asymmetry in many digital services becomes particularly large because most users cannot accurately ascertain the risks of exposing their privacy. If a user is asked to trade their personal data for a short-term financial benefit, such as a discount, the actual cost of the trade-off is difficult to grasp. In this case, the short-term gain (discount) is tangible and immediate, while the potential loss (privacy) long term'.[51]

[51] https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf p7

Data that is shared for commercial purposes may therefore lead to the commercial exploitation of children because they are not receiving sufficient recompense for the use of their data.

3.10.2 Policy objective

To ensure that services give proper consideration to the consequences of, and the reason for, data sharing before they disclose any data, to reduce harms arising from sharing, such as the commercial exploitation of children.

3.10.3 Costs to providers of ISS

Services which already limit data sharing will incur no additional costs.

Other services may incur costs in reviewing their existing data sharing arrangements to make sure that they conform to this standard.

Services which rely upon sharing or selling personal data to fund business models may see a significant drop in revenue. However the available evidence has not allowed us to estimate these effects.

3.10.4 Wider costs

Businesses or organisations which rely upon the supply of personal data may find it more difficult to source. This may in turn affect their functioning and/or business models.

3.10.5 Benefits to providers of ISS

Limiting sharing of children's data should make services more attractive to users, become a selling point and prevent reputational damage to providers. It should also improve trust and confidence amongst users.

3.10.6 Wider benefit

This should reduce the potential for harms to children that are not inherent in the original processing but arise because of the way that and purpose for which the third party processes their personal data. Reducing harms to children should improve outcomes for them and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.10.7 Categorisation of impact

Article 5 GDPR contains an explicit requirement that data should be collected for specified explicit purposes and not further processed in a manner that is incompatible with those purposes. We therefore consider this obligation to be explicit in the GDPR and therefore cost **neutral** for the AADC.

3.10.8 Option considered but not taken forward

None.

3.11 Standard 10 – the need to switch geolocation options off by default, provide a sign when location tracking is active, and default options which make a child's location visible to others off at the end of each use

3.11.1 The issue/problem to be addressed

The ability to track the physical location of children can give rise to risks to their physical safety. This may be particularly problematic if the child's location is made available to the world at large. It can expose children to risks such as abduction, sexual abuse and trafficking. It can also lead to general privacy intrusion by allowing others who are not bad actors to see a child's movements without the user actively deciding they wish to reveal this information.

ICO research in 2019 found seven of 10 parents wanted geolocation services switched off by default when their child first gets an online account, with some variation between types of accounts (67% for music, 70% for social media and 75% for video streaming). 81% of parents felt that geolocation should be switched off by default for targeting children with online adverts, and 83% when geolocation was used for sharing their child's location with other apps, websites and games. In the latter case, half of parents did not want an option for their children to change the settings.[52]

[52] Towards a better digital Future, ICO/Revealing Realities 2019, p20. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf

3.11.2 Policy objective

To ensure that children are not exposed to harms to their health and wellbeing resulting from non-essential use of geolocation data being 'on' by default.

3.11.3 Costs to providers of ISS

Costs are likely to be incurred in re-designing services to default back to off after each use and to provide an obvious sign when tracking is live.

Where income streams are reliant upon geolocation options that are not essential to the service being on by default businesses may see reductions in revenue. However, due to uncertainty and the context-specific nature of these costs it has not been possible to estimate them.

3.11.4 Wider costs

There will be a cost to the ICO in providing appropriate support and advice and assessing conformance to this standard in the event of an investigation.

3.11.5 Benefits to providers of ISS

Providing a child-friendly service should make services more attractive to users, become a selling point and prevent reputational damage to providers. It also aids in achieving data minimisation, as explained above.

3.11.6 Wider benefits

Children will benefit by not being exposed to risks arising from their physical location being shared with others by default. Reducing harms to children should improve outcomes for them and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.11.7 Categorisation of impact

To the extent that geolocation services use '**location data' as defined by PECR** (this is a narrower definition than geolocation data) consent to processing is already required so the requirement to have such options off by default will be **impact neutral** in terms of the code and is only likely to affect a small number of organisations.

Where 'location data' as defined by PECR isn't in use, although this standard links back to underlying fairness requirements of 5(1) it is the

code that makes this an explicit requirement and the Commissioner therefore considers this to be an **incremental impact of the AADC.**

3.11.8 Option considered but not taken forward

None.

3.12 Standard 11 – the need to ensure that when parental controls are provided, children get an obvious sign that their online activity is being monitored

3.12.1 The issue/problem to be addressed

Although parental controls bring benefits in terms of child safety online, they also have privacy implications for children. Children who are subject to persistent parental monitoring may have a diminished sense of their own private space which may affect the development of their sense of their own identity. This is particularly the case as the child matures and their expectation of privacy increases.

3.12.2 Policy objective

To ensure that children are aware of when they are being monitored and can develop a healthy sense of their own identity by being afforded an age appropriate level of privacy.

3.12.3 Costs to providers of relevant ISS

Where this standard is not already met, costs are likely to be incurred in re-designing services to provide an obvious sign that online activity is being monitored.

3.12.4 Wider costs

Some parents may consider that their capacity to protect their children (by monitoring them without their knowledge) has been decreased.

3.12.5 Benefits to providers of ISS

This feature may be valued by child users of services and increase brand loyalty and trust.

3.12.6 Wider benefits

Healthy development of children's sense of identity should lead to a future generation of well-balanced and emotionally resilient adults. It may also

lead to conversations between parents and their children about their safety and encourage more trust.

3.12.7 Categorisation of impact

Although this links back to underlying fairness requirements of 5(1) it is the code that makes this an explicit requirement. The Commissioner therefore considers that the need to ensure that children have an **obvious sign that their online activity is being monitored** is an **incremental impact** of the code.

3.12.8 Option considered but not taken forward

The Commissioner considered the option of requiring ISS providers within scope to provide parental controls and of further requiring them to put options to change children's default privacy settings behind a parental control mechanism. She rejected this option, however, on the basis that there is already a healthy provision of parental controls and that requiring parental authorisation for children to change default privacy settings could in itself be detrimental to the healthy development of children's age appropriate autonomy.

3.13 Standard 12 - the need to switch options which rely upon profiling off by default and to only allow profiling if suitable measures are in place to protect children from harmful effects

3.13.1 The issue/problem to be addressed

There is currently extensive use of profiling by online services whether for the purposes of behavioural advertising or in order to personalise services in other ways. Children are unlikely to understand the ways in which their personal data is being used or the consequences of that use, and sometimes will not be aware that it is happening. Profiling can also lead to children being fed or served up inappropriate content which is detrimental to their health and wellbeing.

3.13.2 Policy objective

To ensure that children are not profiled without them realising it is happening and to prevent profiling leading to harms to children, such as being exposed to inappropriate content.

3.13.3 Costs to providers of ISS

Cost may be incurred in re-coding services so profiling is off by default.

Where business models rely upon profiling being on by default, businesses may see a drop in revenue. For profiling carried out for the purposes of behavioural advertising stakeholders have indicated that this is likely to be a highly significant cost that may render services no longer profitable/viable.

Significant costs may also be incurred in developing algorithms that protect children from harmful effects arising from profiling (such as being fed inappropriate content).

Where profiling is core to the ability to deliver the service, businesses are not required to turn profiling off by default and so no costs will be incurred.

There may be some instances where profiling is used for other purposes than behavioural advertising for services that are not core, and where a lawful basis other than consent is relied upon. While we have not to date seen examples of these from stakeholders, in this instance there would be likely to be some costs associated with re-designing services so this is off by default.

3.13.4 Wider costs

Children who do wish their personal data to be used for the purposes of behavioural advertising or profiling for other purpose will incur additional effort in amended default settings.

3.13.5 Benefits to providers of ISS

Providing a child-differentiated service could make services more attractive to users, become a selling point and prevent reputational damage to providers.

3.13.6 Wider benefits

Reducing the risks of children being exposed to inappropriate content or other personalisation should lead to better outcomes for children and a reduction in harms. This should improve outcomes for children and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.13.7 Categorisation of impact

The opinion of the European Data Protection Board on the interaction between PECR and GDPR requirements confirms that the only appropriate basis for profiling in the context of behavioural advertising is consent. As consent cannot, by definition, be provided by default, the cost to businesses of adopting a '**behavioural advertising off by default'** model is considered to be an existing requirement of the GDPR and therefore **impact neutral** for the code. It is this area where we believe the highest costs will be incurred.

In instances where there is **other, non-core profiling** (which isn't related to processing for the purposes of behavioural advertising and where a lawful basis other than consent is relied upon), the need to switch options which rely upon profiling off by default is made an explicit requirement by the code and the Commissioner therefore considers it to be an **incremental impact** of the code.

3.13.8 Option considered but not taken forward

None.

3.14 Standard 13 – the need to avoid the use of nudge techniques to encourage children to provide unnecessary data or lower privacy settings

3.14.1 The issue/problem to be addressed

Some online services currently use nudge techniques to lead or encourage children to provide their personal data or lower their privacy setting when they wouldn't otherwise do so. This can lead to the commercial exploitation of children or to them being exposed to other harms.

The Norwegian Consumer Council's 2018 study *Deceived by Design* found that, "service providers employ numerous tactics in order to nudge or push consumers toward sharing as much data as possible." It also found that, "privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users."[53]

[53] *Deceived by Design*, Norwegian Consumer Council 2018. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

3.14.2 Policy objective

To protect children from commercial exploitation and other harms arising from the use of their personal data.

3.14.3 Costs to providers of ISS

Costs may be incurred in re-coding services to eliminate existing use of nudge to encourage provision of data or lower privacy settings.

Where business models rely upon the use of personal data for funding, services may see a reduction in revenue. However, given the uncertainty and the context-specific nature of these costs it has not been possible to estimate them.

3.14.4 Wider costs

None identified.

3.14.5 Benefits to providers of ISS

Providing a child-friendly service should make services more attractive to users, become a selling point and prevent reputational damage to providers.

3.14.6 Wider benefits

This should reduce children's exposure to privacy harms, and to other harms arising from use of personal data collected via nudge techniques. This should improve outcomes for children and in turn have a wider societal benefit in reducing costs associated with supporting children who experience difficulties with their mental and emotional wellbeing and in raising future generations of well-balanced emotionally resilient adults.

3.14.7 Categorisation of impact

Although this obligation is linked back to underlying fairness requirements of Article 5(1) GDPR it is the code that makes this an explicit requirement and the Commissioner therefore considers this to be an **incremental impact** of the code.

3.14.8 Other options considered but not taken forward

As this area was not included in the list of suggested areas for inclusion in the code provided by Government, the Commissioner considered omitting it. However, taking into account research into this issue conducted by the Norwegian Consumer Council evidence, she felt it was important to address this practice.

3.15 Standard 14 – the need to ensure that connected toys and devices comply with the requirements of the code

3.15.1 The issue/problem to be addressed

Connected toys raise particular issues because their scope for collecting and processing personal data through functions such as cameras and microphones is considerable, and they are often used by very young children without adult supervision.

3.15.2 Policy objective

To ensure that providers of connected toys and devices give proper consideration to the risks associated with children inadvertently providing their personal data through play. Ultimately this should protect children from various risks of harm (see section 2.1 'Problem under consideration' for further detail).

3.15.3 Costs to providers of ISS

The UK toy industry is the largest in Europe, with a direct contribution to UK GDP of £1.4 billion in 2018. The British Toy and Hobby Association has 138 members which account for 85% of branded toys sold in the UK. SMEs account for 80% of UK toy companies.[54] Connected toys make up less than 1% of toys sold. A speculative market survey by Juniper Research anticipates that global sales of connected toys could reach $18 billion by 2023.[55]

There may be particular costs over and above those detailed in other standards for connected toys and devices given that these are related to the production of a physical product. This could include changes to the packaging and in some cases to the product itself. Innovative approaches will be required to deliver transparency via a physical rather than a screen based product.

[54] British Toy & Hobby Association, AADC consultation response 2019. https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260198/btha.pdf
[55] Connected toys and the Internet of Things, British Toy and Hobby Association, 2019. https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-grow-almost-200pc-by-2023

3.15.4 Wider costs

This standard applies the other requirements of the code in this particular context. Therefore, any of the wider costs detailed under other impacts may apply here.

3.15.5 Benefits to providers of ISS

Any of the benefits to providers of online service within scope detailed under other impacts may apply here, given that this standard applies the other requirements in the code to this particular context.

3.15.6 Wider benefits

Any of the wider benefits detailed under other impacts may apply here, given that this standard applies the other requirements in the code to this particular context.

Benefits are likely to be particularly significant given the potentially privacy intrusive nature of connected toys which may capture individuals' data without their knowledge and are often used by very young children without parental supervision.

3.15.7 Categorisation of impact

This will depend on which requirements of the code are relevant.

3.15.8 Other options considered but not taken forward

The Commissioner considered not including a specific standard on this subject on the basis that organisations should be able to apply the other requirements in the code to the specific circumstances of their product and the data processing involved in delivery. However, stakeholder feedback suggested that there were particular issues to consider for connected toys and devices which warranted a bespoke standard.

3.16 Standard 15 – the need to provide age appropriate online tools

3.16.1 The issue/problem to be addressed

Many services do not currently provide age appropriate tools to help children exercise their data protection rights. This means that when children experience problems with the processing of their personal data they may not have the necessary skills and resources to get any issues

satisfactorily resolved and they may continue to be exposed to harms because they don't know how to stop their personal data being processed.

3.16.2 Policy objective

To empower children to easily resolve any issues they have and help them to exercise their data protection rights.

3.16.3 Costs to providers of ISS

Where services don't have existing online tools new ones may need to be developed.

It may be necessary to develop different tools suitable for different age groups.

3.16.4 Wider costs

None identified.

3.16.5 Benefits to providers of relevant ISS

Providing child-friendly online tools could be seen as a selling point and provide commercial advantage.

Innovating to provide tools to allow users to exercise more control directly may also reduce the level of resources required to respond when they exercise their information rights.

3.16.6 Wider benefits

Adults may also benefit from accessible, easy to use and understand tools for exercising their data protection rights.

Making it easy for children to exercise their data protection rights may lead to an increase in how often this happens, allowing children to have greater control over their own personal data and resolve any issues that arise.

It is also likely to help parents by facilitating their role in educating their children and supporting them in building digital resilience. It may also support teachers in educating children about digital literacy and how to protect and manage their online interactions.

3.16.7 Categorisation of impact

S123 DPA 2018 requires the Commissioner to have regard to the fact that children have different needs at different ages. This makes it clear that it

is not sufficient to just consider the needs of children as one homogeneous group, which gives rise to the potential need for different versions of information or different messaging as a direct impact of the wording of s123 DPA 2018. The Commissioner therefore considered the **need to meet the online tools standard** to be a direct impact of s123 of the DPA 2018.

3.16.8 Other options considered but not taken forward

None.

Annex A: the derivation of the impacts of the standards in the code

The table below summarises in visual form where she considers each impact derives from; many are of mixed derivation and will therefore have a cross in more than one column of the table.

Impact/standard	Counterfactual- Explicit GDPR requirement	Counterfactual- other regulatory requirement	Counterfactual – requirement of s123 DPA 2018	Incremental impact of the code
The scope of the code			X	
Best interests of child			X	
Data Protection Impact Assessments	X			X
Age appropriate application	X		X	
Transparency			X	
Detrimental use of data		X		X
Policies & community standards		X		X
Default Settings	X			X
Data minimisation	X			
Data sharing	X			
Geolocation	X			X
Parental controls				X
Profiling	X			X
Nudge techniques				X
Connected toys and devices	X		X	X
Online tools			X	