**ICO Answer to the call for submissions of the UNSRP**

*‘A Better Understanding of Privacy: Children’s right to Privacy’*

*[Call](https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_July_SRP_Call_for_Submissions_and_Note.pdf) for Submissions*

The Information Commissioner has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst others.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

The Information Commissioner’s Office (ICO) welcomes this opportunity to contribute to the UNSRP’s consultation on children’s privacy and particularly to explain our regulatory approach to tackling some of the key issues, encapsulated in the ICO’s Children’s [Code](https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/) (officially the Age Appropriate Design Code) which applies to digital services likely to be accessed by children and that came into force on 2 Sept 2020.

The ICO is currently the Chair of the Global Privacy Assembly (GPA). We note that the GPA and its Digital Education Working Group, Chaired by our colleagues at the CNIL, have also been working on the topic of children’s right to privacy in detail. The upcoming GPA closed session is intending to adopt the Annual Report of the Digital Education Working Group, expected to reference a presentation of a 2020 study report on legal frameworks in relation to the exercise of children’s rights.

The ICO’s Deputy Commissioner also chairs the OECD Working Party on Data Governance and Privacy. The OECD is drafting a recommendation on Children in the Digital Environment which is also worth mentioning as a global standard in this context.

The call for submissions reads:

*The submissions should relate to the privacy rights of children (under the age of 18) and issues relating to their independence and autonomy in any of the following, or other relevant areas:*

1. *Online and offline in the social, recreational, educational, justice and health spheres;*
2. *Parental, familial, community, governmental, commercial and other interests that influence the development of the child and their autonomy;*
3. *Evidence and/or ongoing research on autonomy of children in educational institutions such as schools taking into account situations including playground, classrooms etc. from age four onwards including impact on perspectives on privacy as expressed by the children themselves;*
4. *Comparative analysis of autonomy and privacy in children taking into account cultural contexts and differences (if any) between attitudes towards and perceptions of autonomy and privacy that may be observed in different regions of the world or between various sub-groups including ethnic, racial and religious.*
5. *Official identity recognition including but not limited to birth registration and other official identity papers;*
6. *The development of personal identity (or ‘self’) including gender identity and expression;*
7. *The sexual development of the child and the importance of private spaces for the child, both on-line and off-line in which one’s sexuality can be further explored;*
8. *The strengths and challenges of ‘age based’ and ‘age verification’ approaches;*
9. *Governmental or other structures including regulatory arrangements, established to advance the human rights of the child;*
10. *Children in vulnerable situations such as unaccompanied migration, violence, sexual exploitation, poverty and other economic, social, familial or physical circumstances;*
11. *Programs, mechanisms and strategies that aid the positive development of the child by addressing their privacy needs and expectations.*

The following response addresses issues relevant to points 1, 2, 3, 6, 7, 8, 10 and 11 above. The five points below are taken together. We have given individual answers to the points 8, 10 and 11.

1. *Online and offline in the social, recreational, educational, justice and health spheres;*
2. *Parental, familial, community, governmental, commercial and other interests that influence the development of the child and their autonomy;*
3. *Evidence and/or ongoing research on autonomy of children in educational institutions such as schools taking into account situations including playground, classrooms etc. from age four onwards including impact on perspectives on privacy as expressed by the children themselves;*
4. *The development of personal identity (or ‘self’) including gender identity and expression;*
5. *The sexual development of the child and the importance of private spaces for the child, both on-line and off-line in which one’s sexuality can be further explored*

The ICO’s response to these five points is structured as follows:

* Children’s use of online services based on research (addressing mainly point 1);
* Harms affecting children’s privacy and data protection (addressing points 1, 2, 3, 6 and 7);
* The Children’s Code (addressing points 1, 2, 3, 6 and 7)

Children’s use of online services based on research

One in five UK internet users are children – but the internet was not designed for them or with safeguards for their data[[1]](#footnote-1) and our own research shows that when children understand what’s going on behind the scenes with their data, they are not happy.

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]](#footnote-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]](#footnote-3).

Parliamentary debate during the passage of the UK Data Protection Bill recognised that services are often developed for adult users, with insufficient regard for the consequences for young people. Moreover, 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.

Ofcom’s 2019 Children’s Media Use and Attitudes research also found that children often use online services whilst on the go and away from parental oversight[[4]](#footnote-4). According to Professor Sonia Livingstone, “even the oldest children struggle to comprehend the full complexity of internet data flows and some aspects of data commercialisation”[[5]](#footnote-5).

Harms affecting children’s privacy and data protection

In the UK Commissioner’s view the key harms to children that can arise from the processing of their personal data online are:

* Privacy intrusion and data protection (including loss of autonomy and damage to personal reputation);
* Harms to children’s mental and emotional health and wellbeing, physical harms; and
* Economic harms or commercial exploitation.

The following sections give further details on each of these three key harms affecting children’s privacy and data protection.

*Privacy intrusion and data protection*

Ensuring that children can 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[[6]](#footnote-6).

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.

To inform the development of the Children’s Code, the ICO commissioned external research with children and parents to explore their views on privacy, data protection and links to autonomy. For example, the final report, based on qualitative and quantitative data, ['Towards a Better Digital Future'](https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf) found that:

* faced with a choice between privacy protection and access to an ISS the fear of missing out often outweighed concerns over data privacy;
* children felt that they had to give away their data to get access to the service;
* many children felt uncomfortable sharing personal data when they couldn’t understand why the platform was asking for it; and
* few younger children understood that adverts could be targeted at them based on their user history or search data.

*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 are processed can also increase their exposure to other kinds of harm. Personal data processing can lead to, or exacerbate, wider harms such as online bullying, abuse and exposure to content leading to anxiety, self-harm or eating disorders. For instance, if children’s personal data is used to inform content feeds, suggest contacts, or keep children online, this could result in harm to their physical and emotional wellbeing as well as their mental health[[7]](#footnote-7).

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)[[8]](#footnote-8).

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.

*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[[9]](#footnote-9).

A 2016 EU study of the impact of online marketing 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[[10]](#footnote-10).

Nudge techniques and micro-transactions in games and mobile applications are common, often designed to be hard for young people to resist. Techniques such as 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)[[11]](#footnote-11)not only result in obvious direct economic harm (children spending money) but also mean children’s data is used for financial gain of a commercial enterprise with no or insufficient recompense to the child (or without the child even knowing it is happening)[[12]](#footnote-12).

The Children’s Code or Age Appropriate Design Code

Recognising the need for action to tackle risks to children posed by online services processing their personal data and to empower young people as users, the UK Parliament placed a duty on the Information Commissioner to create the Children’s Code in section 123 of the Data Protection Act 2018. The aim was 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. Section 123 also directed the Commissioner to have regard to the UK’s obligations under the UN Convention on the Rights of the Child.

The code is rooted in data protection legislation and translates legislative requirements into design standards for online services, helping businesses to understand what is expected of them. It puts children at the centre of design and development and it compels organisations to consider the best interests of the child when using their data. The aim is not to protect children *from* the digital world, but to protect them *within* it; by ensuring that services are better designed with children in mind, both protecting and empowering them as users.

*Scope of the code*

The code applies to ‘[information society services’](https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/?q=analytics) or ISS likely to be accessed by children in the UK. In simple terms, that means many apps, online games, connected toys and devices, search engines, social media platforms and websites that offer goods, news or education services. It is not limited to services specifically directed at children.

*Key standards of the code*

The code’s 15 design standards are cumulative and, when applied together, ensure that children receive an age appropriate service that recognises that they merit specific protection with regard to the processing of their data. The code sets out how organisations can design their services to recognise the shifting needs of children at different development stages.

**Best interests of the child**

The code incorporates the key principles from the United Nations Convention on the Rights of the Child (UNCRC). The first standard mandates that the best interests of the child should be a primary consideration when designing and developing services likely to be accessed by children.

It aims to respect the rights and duties of parents, and the child’s evolving capacity to make their own choices. In particular, it seeks to ensure that online services use children’s data in ways that support the rights of the child with regard to: freedom of expression; freedom of thought, conscience and religion; freedom of association; privacy; access to information from the media (with appropriate protection from information and material injurious to their well-being); to play and engage in recreational activities appropriate to their age; and protection from economic, sexual or other forms of exploitation.

This includes how ISS can ensure that their data processing supports children’s physical, psychological and emotional development as well as their need to develop their own views and identity. The standard also acknowledges that the best interests of the child have to be balanced against other interests (for example interests of other children).

**Transparency, policies and community standards**

The code obliges services to provide clear, concise and prominent transparency information, terms, conditions and community standards. ‘Bite-sized’ explanations of how the service will use personal data should be provided at the point use is activated. This is key to ensuring that data is processed fairly and that children understand what is happening with their data and, as they develop greater autonomy, can make more informed choices about which services they use and what information they choose to share.

Services must also uphold published terms, policy and community standards, which includes privacy policies, age restrictions, behaviour rules and content policies, to ensure that they are processing data fairly.

**Detrimental use of data**

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.

The code states that services must not use children’s personal data in ways that have been shown to be detrimental to their wellbeing or that go against industry codes of practice and other regulatory provisions of Government advice.

**Default settings, profiling, geolocation, nudge techniques, parental controls**

Default settings must be ‘high privacy’ by default (unless a compelling reason for a different default setting can be demonstrated, taking account of the best interests of the child). This offers children greater protection so that if they do nothing when they start using a service their data is protected automatically, by design and by default. It also supports data minimisation and greater user control.

Where settings are changed services must ensure that child users are properly informed and supported and that they still receive an age appropriate service. So, for example, content feeds should only recommend appropriate material or targeted adverts suitable to the age of the user.

Profiling should be ‘off’ by default (unless services can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Services can only use profiling if they have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

Geolocation options should also be off by default (unless the ISS can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Children should be provided with an obvious sign when location tracking is active and options which make a child’s location visible to others must default back to ‘off’ at the end of each session.

Nudge techniques must not be used to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.

Where parental controls are made available, services should give the child age appropriate information about this. If the online service allows a parent or carer to monitor their child’s online activity or track their location, an obvious sign should be provided to the child when they are being monitored. This standard further supports the autonomy of the child. The code provides further details on how this standard can be met based on the age of the child.

**Online tools**

This standard addresses children’s ability to exercise their information rights. Services should offer prominent and accessible tools to help children exercise those rights and report concerns. This encompasses [the](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/) right of access, [rights to rectification,](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/) [erasure and](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/) portability as well as rights to object, restrict processing, and [rights related to automated decision making.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/)

Our response now addresses items 8, 10 and 11.

*8. Strengths and challenges of ‘age based’ and ‘age verification’ approaches*

Understanding the age range of children likely to access a service, and the different needs of children at different ages and development stages, is fundamental to the whole concept of age appropriate design.

The age appropriate application standard in the Children’s Code explains that services can choose to establish the age of a user with a level of certainty that is appropriate to the risks to the rights and freedoms that arise from its data processing and then apply the code to child users only or apply the standards in the code to all users. This should mean that, even if services don’t really know how old a user is, or if a child has lied about their age, children still receive some important protections.

The code is not prescriptive about the methods services should use to establish age, or what level of certainty different approaches offer. This is because this will vary depending on the specifics of the techniques used. It is also important to allow enough flexibility for services to use measures that suit the specifics of their individual service and that can develop over time. However, approaches should always be appropriate to the risks that arise from the data processing.

Some of the methods that can be used to establish age are set out in the code and include: self-declaration, artificial intelligence, third party age verification services, use of account holder confirmation, technical measures and, in some circumstances, collection of hard identifiers taken from official documents like passports. The ICO recognises that methods of age assurance will vary depending on whether the service is used by authenticated or non-authenticated users (eg. whether users are logged in) and that the risks may also vary in this context.

The code also explicitly states that services cannot simply re-purpose information collected for age assurance. The Commissioner recognises that there is tension between age assurance and compliance with compliance with data protection legislation, as the implementation of age assurance could increase the risk of intrusive data collection. However, the code does not require organisations to create these counter risks and the two are compatible if privacy by design solutions are used.

The code also notes that age assurance tools are still a developing area and the Commissioner has committed to work to establish clear industry standards and certification schemes to assist children, parents and online service in identifying age assurance services which comply with data protection standards.

*10. Children in vulnerable situations such as unaccompanied migration, violence, sexual exploitation, poverty and other economic, social, familial or physical circumstances*

The code aims to ensure that services likely to be accessed by children are designed with built in protections. In part, this is in recognition of the fact that not all children have engaged parents or carers who can act in their best interest to protect and support them in their engagement with digital services.

Children with additional needs

In the 2019 Report that was commissioned by the ICO (referenced above), the research showed that:

* Parents and carers of children with additional needs favoured high privacy settings by default
* Parents and carers of children with autism and learning disabilities also believed that decisions about online privacy needed to be made on behalf of their children rather than by them.
* Parents and carers of children with disabilities felt that their children were more vulnerable to targeted advertising.

The code acknowledges that children with disabilities may have additional needs and that services should consider any additional responsibilities they may have under applicable equality legislation.

This should be considered when undertaking a Data Protection Impact Assessment. It is also explicitly referenced in the best interest of the child standard and age appropriate application. The profiling standard also recognises that there may be exceptions where it is appropriate for profiling to be on by default, such as where this is necessary to ensure a service is accessible to a disabled child.

*11.**Programs, mechanisms and strategies that aid the positive development of the child by addressing their privacy needs and expectations*

The Code’s status and regulatory approach

The Children’s Code is a statutory code of practice. It has successfully completed the UK Parliamentary approval process and came into force on 2nd September 2020. However, there is now a 12 month transition period for organisations to bring their services into conformance. The Commissioner will assess conformance with the code from 2 September 2021. In line with good regulatory practice, she has also committed to review the code in Autumn 2022 to ensure that it is delivering the changes that were intended and to assess whether organisations require any further support.

In accordance with section 127 of the UK Data Protection Act, the Commissioner and the courts must take the code into account when considering whether online services likely to be accessed by children have complied with their data protection obligations, to the extent that it is relevant. Organisations that don’t conform to the standards are likely to find it more difficult to demonstrate that their processing is fair and complies with data protection requirements. In the meantime, if a child’s data is processed in a way that infringes data protection legislation the ICO can take action. We can issue assessment notices, warning, reprimands, enforcement notices and administrative fines. In the most serious cases where the data protection principles are infringed, we can issue penalties of up to 4% of annual worldwide turnover.

The code is clear that we will take a risk based and proportionate approach to our oversight of the code, in line with the ICO’s regulatory action policy.

ICO’s support to implement the Code

To ensure that the code is successfully implemented the Commissioner is developing a package of support for industry to support them in making the necessary changes to their services. This includes a new Children’s Code hub which houses frequently asked questions and practical tools to explain the code. The ICO is also running a series of introductory webinars, in collaboration with industry, as well as developing more detailed workshops to explore different aspects of the code, such as the concept of risk and assessing the best interests of the child.

The ICO is also offering support to organisations implementing the code via its Regulatory Sandbox. This offers innovators the possibility of concentrating on cutting edge personal data projects dealing with issues posed by the Children’s Code. The Sandbox designed to support organisations using personal data to develop innovative products and services and accepts applications from all types of organisations from start-ups, SMEs and large organisations, across private, public and voluntary sectors.

Organisations seeking practical advice and support on the code can also access it from the ICO’s innovation hub.

Further information about this support programme is available in the following ICO [link](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/09/ico-s-children-s-code-will-help-protect-children-online/).

All future developments about the Children’s code will be announced on the ICO’s website [hub](https://ico.org.uk/for-organisations/childrens-code-hub/).

1. Introduction to the Children’s Code, 2020, ICO https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/ [↑](#footnote-ref-1)
2. Online Nation 2020 Report, Ofcom, p34-37. [↑](#footnote-ref-2)
3. Online Nation 2020 Report, P40. https://www.ofcom.org.uk/\_\_data/assets/pdf\_file/0027/196407/online-nation2020-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. [↑](#footnote-ref-3)
4. 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 [↑](#footnote-ref-4)
5. Children’s data and privacy online: Growing up in a digital age, p4 [↑](#footnote-ref-5)
6. Peter and Valkenburg, 2011; Raynes-Goldie and Allen, 2014; Pradeep and Sriram, 2016; Balleys and Coll, 2017. [↑](#footnote-ref-6)
7. ICO Impact Assessment for the Children’s Code, 2019, p.13-14, https://ico.org.uk/media/2617988/aadc-impact-assessment-v1\_3.pdf [↑](#footnote-ref-7)
8. Ibid. [↑](#footnote-ref-8)
9. Ibid. [↑](#footnote-ref-9)
10. 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 [↑](#footnote-ref-10)
11. The Rip-off Games, Parent Zone 2019. p9. https://parentzone.org.uk/the-rip-off-games [↑](#footnote-ref-11)
12. Ibid. [↑](#footnote-ref-12)