Submission on behalf of the British Broadcasting Corporation

1. The BBC welcomes the opportunity to submit evidence to the Information Commissioner with regards to the Age Appropriate Design Code (the **Code**), required pursuant to the Data Protection Act 2018 (**DPA 2018**).

2. The BBC is submitting evidence to this inquiry as a Public Service Broadcaster (PSB), an organisation that provides world-class, impartial and accurate news, children' s services and a major provider of internet content and services. We have addressed the areas which are most relevant to the BBC.

3. The BBC has a public mission to inform, educate and entertain. The BBC recognises that the internet has significant potential to help us fulfil this mission, notably with regards to services designed for children. This was acknowledged by government in the Internet Safety Strategy Green Paper, which states that the BBC' s online services provide a *"safe, trusted space where [children] can learn, create and have fun in one place ... We will engage with the BBC as they support and promote child online safety and digital literacy through BBC Children's Stay Safe initiative, helping UK children become among the most digitally literate and resilient in the world."* [1]

4. The BBC is mindful in the context of children' s exposure to the Internet, that such access raises legal, technological and ethical considerations that require careful consideration. We therefore welcome the Code as an important opportunity to:
   - o identify the guiding principles for Government, industry and civil society groups, that can act as a reference point for now and in the future; and
   - o in so doing, provide an appropriate governance structure for the processing of personal data.

Executive Summary

5. The BBC seeks to provide something for everyone in the United Kingdom: a service which is easily accessible, without unnecessary barriers and excessive processing of personal data. This includes young persons. To do so, we implement high security and

---

[1] *https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper p33*

privacy standards and we work every day to maintain and build upon trust to make the BBC a safe place for everyone regardless of age.

6. We consider that privacy by design, transparency and accountability are the key concept that the Code must be based around. Robust childhood privacy impact assessments, tied always to the data protection principles and concept of accountability would:

    a) serve as a reminder of the special importance and roles, the freedoms and privileges, the power and responsibilities of data processors; and

    b) provide a full context for the choices which fall to be made in practice so that they can be made in accordance with the principles to be derived from this context.

7. The BBC views the Code as an opportunity to create an *accountability-centric Code*, as opposed to a quasi-legislative *design manual. This would provide the accountability that the system needs but also provide flexibility to enable services to* grow and develop in the future.

8. This would be consistent with the scope and remit of Code located within all of the accountability obligations incumbent upon organisations and the powers of the ICO, within the scope of the requirements and principles of both the DPA 2018, the Human Rights Act 1998, the UN Convention on the Rights of the Child and the GDPR. The BBC warmly welcomes the Code as an opportunity to devise a principles based, accountability centric framework for the processing of children's personal data.

9. The assessment should take into account age-appropriate rights and freedoms of the child so that their freedom to learn, develop and explore (particularly in an online context) is only restricted when this is a reasonable safeguard. For example, this could mean:

    a) designing processing so that it provides sufficient protection for children;

    b) taking appropriate actions to enforce any age restrictions you have set; or

    c) implementing up-front age verification processes e.g. requiring parents to verify that they have parental responsibility and to confirm the age of their child.

10. This approach would help ensure the Code is enduring, authoritative and respected. It would have consequences in terms of how individuals and organisations are perceived,

in terms of rewards and sanctions. The Code should encourage organisations to have honest and open discussions, working with the ICO.

11. There have been suggestions that there needs to be more rules on the Code, governing the mechanisms as to how data is processed, rather than a general guidance on accountable design. Robust impact assessments, minimising data collection and a commitment to data security make sites safe. The choice of solutions may vary depending upon the risks inherent in the processing, the rights and freedoms of the child, the particular provisions of data protection law that apply to the processing undertaken and the available technology.

12. The downsides of this approach are that it could create a culture of box ticking, rule bending, loop-hole lawyering and buying compliance rather than engaging with risk in an accountable way. Nor does such an approach take into account the pace and breadth of technological innovation. It runs a risk that compliance could be bought with the right third party system plug-in, drafting terms that disclaim all responsibility and places risk back onto the end user (or their parent) if they fail to appreciate the risk coding system.

13. Though stated in a general GDPR context, we observe that the Information Commissioner herself has previously stated: *"the new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."* [2]

The Structure of this Submission

14. The BBC is happy to play its role in developing this framework and in so doing, offers some observations on the Code. We have grouped our response into three key areas:

   i.   The wider market and the BBC's role.

   ii.   Specific issues

   iii.   The DPA 2018 and the Code

---

[2]   *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/information-commissioner-talks-gdpr-and-accountability-in-latest-speech/*

1. THE WIDER MARKET AND THE BBC'S ROLE

The Market

15. In our view, as part of this consultation, it would be unhelpful to attempt to identify and single out specific companies as disruptors. The environment and the players are constantly changing and later entrants into the market who will be benefiting from technological advancements - artificial intelligence and machine learning – are likely to be as disruptive as the first and second generation technology disruptors. For this reason, the BBC seeks to work closely with the ICO to support appropriate measures to protect children.[3]

16. Whilst the BBC, as a public service provider, see no contradiction or dissonance with being technologically advanced, innovative and to a significant degree, being dynamic players seeking to innovate in the online digital space: technology disruptors are, as alluded to above, distinct in substance and in form from the BBC. We are therefore mindful that interventions and solutions proffered through this consultation should strike an appropriate balance showing awareness and sensitivity to the varying purpose of service providers.

17. The BBC also provides its submission in the context of the Government's policy to build digital capability across the economy. This has included significant investment to improve digital education at primary and secondary levels, as well as making digital skills training for adults a statutory right from 2020. In higher education, government-backed initiatives like the Alan Turing Institute have helped set the UK apart as a world-leading research base for data science and innovation, while substantial funding for new PhDs

---

[3] *Technological innovators have by definition been ahead of the curve in gathering and mining extensive amounts of personal data. Over the past 10 -15 years, there has been an exponential growth in technology companies – companies who in some cases make significant use of personal data to maximise the effectiveness of their product or services conversion funnels –utilising the internet to 'virtualise' the world, and repurpose it digitally and online. This has largely happened without customers being fully aware of the consequences and the effect of their participation and involvement. The recent focus on Cambridge Analytica has demonstrated an increased awareness of and need for online platforms to be transparent about their business practices and use of personal data.*

and fellowships in AI will help maintain the flow of world-class talent from our universities.

The BBC's Place in the Market

18. The BBC has a unique public service mission derived from its Royal Charter. We aim to harness technology to provide the best service possible for our audiences. The BBC's approach to data and the processing of personal data is informed by our public service remit which is non-commercial. We seek to provide information and learning content to provide good public services for its own sake.

19. It is widely acknowledged that the collection and analysis of data is important to provide a personalised service. In the future, the BBC will need to make the most of the opportunities offered by IP delivery to get more, better, personalised content and services to audiences in order to sustain a thriving UK creative economy. The BBC's privacy policy is clear, transparent and available to read online.[4] It includes specific references to children's protection.

20. In the Internet Safety Strategy Green Paper, the government state that the BBC's online services provide a *"safe, trusted space where [children] can learn, create and have fun in one place ... We will engage with the BBC as they support and promote child online safety and digital literacy through BBC Children's Stay Safe initiative, helping UK children become among the most digitally literate and resilient in the world."* [5]

21. Any industry organisation providing digital services to children should provide information for parents and users about how to engage with the company's services safely. Our guiding principle is that it is for parents to oversee the consumption of our online and digital content but it is our responsibility to provide children and parents with access to the content, information and tools to make these decisions. As outlined in the BBC's submission to the Committee's *Children and the internet* inquiry,[6] this is delivered predominantly through the BBC's policies rather than external regulation,

---

[4] https://www.bbc.co.uk/usingthebbc/privacy-policy/
[5] https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper p33
[6] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/written/40400.html]

though we are accountable to Ofcom for the protection of under-18s in our licence fee-funded television and radio services.[7]

22. The UK has kept the minimum age at which a child is capable of giving consent (if consent is the lawful basis for data processing relied on) at 13. The BBC welcomes this decision which is consistent with the GDPR, the ICO's Consultation on Children's Data. The BBC is also very mindful about how we engage with and respond to children aged 13–16 online. We offer examples of best practice with regards to obtaining parental permissions in Part 3 of this Submission.

23. We welcome the opportunity to advise Government and other partners on our experience of establishing best practice for children's content and services online.

2. SPECIFIC ISSUES

24. We welcome the Code as an important commitment to data protection online; however, it would not be in the best interests of children or content providers if the Code became a vessel through which the internet becomes age-gated, or through which organisations determine that it is not feasible to deliver content to internet users under 16. In this section we highlight issues for further consideration by the ICO.

When a child is 'likely to access a service'

25. BBC apps and other online services specifically for children are designed with appropriate safeguards in place. For example, the new CBBC Buzz app[8] has a team of moderators to approve or decline user-generated content, parental controls and does not allow users the means to make negative comments about other users' content.

26. Online services such as BBC iPlayer have protection systems such as G for Guidance, which not only provides a parental lock, but also offers programme information which replicates the information available for post watershed programmes on TV. When this system was introduced it was offered it to the other UK national PSBs, with the help of Ofcom, which enabled all UK PSBs to have the same system of guidance and pin

---

[7] http://www.bbc.co.uk/editorialguidelines/guidelines/accountability/ofcom
[8] http://www.bbc.co.uk/mediacentre/latestnews/2018/cbbc-buzz

protection. We also use the G for Guidance principles and labelling for our off platform on demand content. We aim to ensure that our judgement on guidance warnings is as up to date as possible, particularly on language, following Ofcom research on changing perceptions on offensive language[9] allowing parents to make good choices about the services their child accesses.

27. The BBC is also a UK-leader in providing advice and guidance to children and their parents on how to navigate online. This includes the *Own It*[10] website (developed from the Stay Safe initiative) which collates BBC and third-party resources for 9-12 year olds to help them stay safe and enjoy their time online. The BBC iPlayer Kids app is the one of the most used and downloaded children' s app the BBC has ever had. As the BBC increase personalisation in the main BBC iPlayer experience it shows an evolution and continued commitment to protecting children online.

28. In contrast to the safe online spaces provided by the BBC, BBC research shows that children and young people have been exposed to negative, harmful or inappropriate content online. One in six 12-15 year olds and one in ten 8-11 year olds who go online had seen something in the past year that was worrying, nasty or offensive.[11] Recent evidence that YouTube Kids contained inappropriate content have further underlined the need for appropriate safeguards for children online.[12]

29. However, age-gating content which isn' t designed for children but which they may access such as BBC Sport, News etc. may not be practical and could add little from a privacy protection angle.[13] Robust impact assessments, minimising data collection and a commitment to data security make sites safe. The choice of solutions may vary depending upon the risks inherent in the processing, the rights and freedoms of the child, the particular provisions of data protection law that apply to the processing undertaken and the available technology.

---

[9] *All BBC content – whether broadcast, online or on BBC channels on social media – is governed by our Editorial Guidelines. These include substantial policies and advice on child protection. We also have very clear guidance about what should appear on the BBC online – for example, any content on or one-click away from the BBC Home would normally be suitable for a general audience.*

[10] *https://www.bbc.com/ownit*

[11] *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/written/40400.pdf*

[12] *http://www.bbc.co.uk/news/technology-43893862*

Data sharing

30. Children's data may not be shared with third parties, unless it is in the best interests of children and we fully support the principle of setting the bar high. We recognise the potential benefits to certain settings being off by default. We would welcome clarification on practical issues such as areas of responsibility – for example, the roles of parent and content provider.

31. To deliver our services we sometimes use service providers. And the services will usually involve the collection and processing of analytics data, some of which is classified as personal data for the purposes of GDPR.[14] For example, our aim is to create a personal connection between the BBC and learners. To do this we wish to use the services of a learning platform provider to help students build their knowledge through participatory experiences. Students will receive notifications via email and mobile, to tell them when they need to come back and practise again - ensuring they know when they need to reaffirm their knowledge. When they return the content will be automatically optimised to ensure they are practising the concepts they are most at risk of forgetting or need reinforced. In order for the BBC to retain and grow our younger audience, customisation and interactivity is key.

Personalisation

32. In order to provide services that meet the needs of the child, this may involve the collection of personal data (where a lawful basis and appropriate fair processing notices have been provided). We welcome the ability to undertake Privacy Impact Assessments to assess the risk of processing, in order to achieve good privacy outcomes. If the requirements with regards to personalisation are overly prescriptive this could impact the BBC's ability to serve audiences better through appropriate personalised services.

33. The BBC is very conscious that it strikes an appropriate balance between personalisation – where it optimises its services for the individual – and providing universal experiences and a shared base of knowledge for UK citizens, and this is embedded into how it designs its services and products.

Online viewing functionality (such as cross device 'Pause' and 'Resume' features)

---

[14] Personal data is typically pseudonymised (e.g. hashed device IDs or IP addresses).

34. This feature requires data collection at an account level (based on sign up to appropriate data protection complaint permissions and fair processing notices), to track where the user has watched a programme to. However, it is seen as a basic provision of service in the current multi-device world. With regards to the provision of internet enabled broadcast and on-demand devices, if such features services are switched off by default this may affect user enjoyment and experience. We consider that this is an issue that should from part of internal privacy impact assessments rather than external guidance.

'Traffic Lights' Systems and Universal Reporting Standards

35. Traffic light and RRP systems can provide an easily understandable flagging system, however, there is a risk that this could lead to a 'box ticking' approach to self-certified compliance and undermine the concept of privacy by design, forcing accountability and the data protection principle to be robustly considered form the outset. The primary rationale for the Code is that it is a *'design* code' not, a system to create a standard. We do however welcome an approach of 'clear labelling' different types of digital spaces including: creative, play, entertainment, education, social and commercial.[15]

Geo-location

The BBC requires such information to check whether someone is in the UK or not (e.g. via IP address).Therefore in limited circumstances where the impact upon privacy has been assessed by organisations, it should be for the organisation itself to make such assessments as to the use of Geolocation.

3. THE DATA PROTECTION ACT 2018 AND THE AGE-APPROPRIATE DESIGN CODE

A Code of Practice for Standards of Age-Appropriate Design

36. It is necessary for the Code to be located within the DPA 2018 and the powers of the Commissioner. The ICO is required pursuant to the DPA 2018 to *"prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age- appropriate design"* .

---

[15] *https://5rightsframework.com/static/Digital_Childhood_report_-_EMBARGOED.pdf*

37. According to the DPA 2018 *"age-appropriate design" means the design of services so that they are appropriate for use by, and meet the development needs of, children"* . The Code goes on to clarify that *"standards of age-appropriate design of relevant information society services" means such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children."* This is the scope of the Code.

38. The Code will have the force of a statutory code. It will be admissible in legal proceedings and in proceedings before a court or tribunal. The Information Commissioner must also take it into account when carrying out her functions in relation to all data protection legislation.

39. How regulation can be effectively applied in its operational context is not a new conundrum and has been extensively considered in the wider context of how to devise effective regulation.[16] As noted by Black, one of the problems associated with the creation of rules in any context, are *"their tendency to over or under inclusiveness, their indeterminacy, and their interpretation"* (Black (2012) p.6).[17] She observes that many of the issues associated with effective regulation stems from the prescriptive nature of rules as *"anticipatory, generalised abstractions"* which when *"endowed with legal status are distinctive, authoritative forms of communication"* . The shortcoming of prescriptive 'rules' is that is seeks to herd certain behaviours and/or attributes, to build up a category and/or definition which then forms a basic rule,[18] which is subsequently used as a net which is thrown over a wide variety of circumstances for which it was not designed to accommodate..[19] As expressed most aptly in the ICOs blog post on children's privacy *"like learning to ride a bike, it is all a matter of finding the right balance between* protecting our children and granting them the freedom to explore the digital world." [20]

---

[16] *See fn 2.*
[17] *The jurisprudential literature on rules is extensive. For legal analyses of rules see in particular F. Schauer (1991); Twining and Miers (1991); Hart and Sacks (1958); Kennedy (1976); MacCormick (1978).*
[18] *Julia Black, Rules and Regulators, Print publication date: 1997, Published to Oxford Scholarship Online: March 2012,*
[19] *John Perry Barlow "The economy of selling ideas": Selling wine without bottles on a global net" available at <http://www.eff.org/EconomyOfIdeas.html> accessed 12 July 2016.*
[20] *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/06/blog-children-s-privacy-call-for-evidence/.*

The Central Importance of the Data Protection Principles, Governance, Privacy by Design and Accountability

40. The BBC warmly welcomes this principles based, accountability centric framework for the Code. We consider that privacy by design, through robust childhood privacy impact assessments, tied always to the data protection principles and concept of accountability would:

    a) serve as a reminder of the special importance and roles, the freedoms and privileges, the power and responsibilities of data processors.

    b) provide a full context for the choices which fall to be made in practice so that they can be made in accordance with the principles to be derived from this context.

41. In our view this approach would allow the Code to be authoritative and respected. It would have consequences in terms of how individuals and organisations are perceived, in terms of rewards and sanctions.

42. In the context of General Data Protection Regulation (the **GDPR**), as stated by the Information Commissioner: *"If businesses are looking beyond the current laws, and are trying to future proof themselves against changing or uncertain legislation, the answer takes us back to accountability."* [21]

43. It would, in short, help providers to understand the circumstances in which they are called upon to make ethical decisions. Crucially it would help them to make the right choices in practice. It would not do this not as a matter of rigid and disconnected prescriptions and prohibitions, but by promoting *"a stable disposition to act in certain ways for the right reasons"* .[22] It would force organisations to recognise and explain the circumstances in which the temptations and motivations to act unethically (including commercial motivations) may be especially strong, and why they need to be resisted, in order to change the incentive structure in such cases.[23]

---

[21] *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/information-commissioner-talks-gdpr-and-accountability-in-latest-speech/*

[22] *http://webarchive.nationalarchives.gov.uk/20140122192214/http://www.levesoninquiry.org.uk/wp-content/uploads/2012/07/Witness-Statement-of-Dr-Neil-Manson.pdf.*

[23] *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/270939/0780_i.pdf page 87.*

44. It is for organisations to look to themselves and undertake risk assessments. Indeed, as noted in the Call for Evidence, "*the Code will further the concept of data protection by design, which is a key feature of the new Data Protection Act and the GDPR*".[24]

45. As with any other processing, fairness and compliance with the data protection principles lies at the heart of all processing of children's personal data. The purpose of these principles is to protect the interests of the individuals and this is particularly important where children are concerned. They apply to everything organisations do with personal data and are key to complying with the GDPR, and by extension the processing of personal data relating to children. [25]

46. We broadly welcome this approach. The benefit to adopting a principles based approach to regulation tied to the DPA 2018 more generally, backed up with examples of best practice, as opposed to devising a prescriptive technical frameworks and series of accreditation schemes which do not exists at the time of publishing the Code, is that it can "*create a community of interpretation of rules through rules themselves*", allowing for the necessary reciprocity between regulator and regulatee.

47. As considered in Part 3 of this Submission, there have been suggestions that there needs to be more rules on the Code, governing the mechanisms as to how data is processed, rather than a general guidance on accountable design. Such examples include introducing traffic lights systems for websites or switching off system functionalities by default. In our view this creates a culture of box ticking and 'buying compliance' rather than engaging with risk in an accountable way. Nor does it take into account the pace and breadth of technological innovation.

---

[24] *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/06/blog-children-s-privacy-call-for-evidence/*

[25] *In the debates on the Data Protection Bill, the Parliamentary Under-Secretary of State, Department for Digital, Culture, Media and Sport (Lord Ashton of Hyde) (Con) stated: "amendment 109 would require the Information Commissioner to produce a code of practice on age-appropriate design of online services.... 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. These are similar to the standards proposed by the noble Baroness [Kidron] in Committee. They include 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, and any other aspect of design that the commissioner considers relevant".https://hansard.parliament.uk/lords/2017-12-11/debates/154E7186-2803-46F1-BE15-36387D09B1C3/DataProtectionBill(HL) See Column 1439.*

48. Put simply it runs a significant risk that compliance can be bought with the right third party system plug-in, drafting terms that disclaim all responsibility and places risk back onto the end user (or their parent) if they fail to appreciate the risk coding system. More disconcertingly it may also encourage a culture that it is easier to deny access to a service than not think about how to mitigate the risks associated with it.[26] Though stated in a general GDPR context, we observe that the Information Commissioner herself has stated: *"the new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."* [27]

Building in Data Protection by Design

49. As stated in the ICO's detailed Data Protection Impact Assessment Guidance: *"A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations...* DPIAs are an essential part of your accountability obligations." [28]

50. Recital 38 of the GDPR states that: *"children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The*

---

[26] Keach, S Brits BLOCKED from websites and video games shut down as GDPR brings chaos to web. https://www.thesun.co.uk/tech/6374543/gdpr-websites-down-eu-not-working/. Novak, M Dozens of American News Sites Blocked in-Europe as GDPR Goes into Effect Today. https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542

[27] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/information-commissioner-talks-gdpr-and-accountability-in-latest-speech/

[28] https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf

consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

51. We welcome the observation by 5Rights and Baroness Kidron that "*Childhood Impact Assessments as standard for all existing services and products, and new services and products prior to launch... Introducing child impact assessments before services and products are rolled out would circumvent some of the most obvious data risks*" .[29]

52. It would, in short, help providers to understand the circumstances in which they are called upon to make ethical decisions. Crucially it would help them to make the right choices in practice. It would not do this not as a matter of rigid and disconnected prescriptions and prohibitions, but by promoting "*a stable disposition to act in certain ways for the right reasons*" .[30] It would force organisations to recognise and explain the circumstances in which the incentives to act unethically (including commercial motivations) may be especially strong, and why they need to be resisted, in order to change the incentive structure in such cases.[31]

53. This approach would seek to provide clarity, and would focus on practical applicability to everyday decision-making. It would not expect to stand alone. It would take its place in a context of ethical culture, sources of advice and guidance both generally and at the particular levels of training, reinforcement, management and feedback. The BBC is also mindful that with regards to the processing of Personal Data, there is a convergence between how all Personal Data is managed. We welcome the Code as an opportunity to acknowledge that every organisation should use an appropriate Data Protection Impact Assessment to assess and mitigate the data protection risks to the child. The BBC has also put in place internal mechanisms to look at how we set policies and standards, and put them into practice, across the BBC.

54. The assessment should take into account age-appropriate rights and freedoms of the child so that their freedom to learn, develop and explore (particularly in an online

---

[29] *Ibid fn 10. 5Rights also suggest that the Commissioner might consider using the Responsible Innovation Framework as defined by the Engineering and Physical Sciences Research Council.*

[30] *http://webarchive.nationalarchives.gov.uk/20140122192214/http://www.levesoninquiry.org.uk/wp-content/uploads/2012/07/Witness-Statement-of-Dr-Neil-Manson.pdf.*

[31] *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/270939/0780_i.pdf page 87.*

context) is only restricted when this is a reasonable safeguard. For example, this could mean:

- designing processing so that it provides sufficient protection for children;
- putting in place proportionate measures to prevent or deter children from providing their personal data (e.g. by placing a note beside a free text field in a quiz reminding users not to put any of their personal data into the box in addition to the quiz answer)
- taking appropriate actions to enforce any age restrictions you have set; or
- implementing up-front age verification processes e.g. requiring parents to verify that they have parental responsibility and to confirm the age of their child.

ENDS