UNIVERSITY OF CAMBRIDGE

CAMBRIDGE PRO BONO PROJECT

CHILD RIGHTS IN A DIGITAL WORLD

A report on the legal process of implementing UNCRC general comment No. 25 (2021) on children's rights in relation to the digital environment in the UK

A research paper for

5RIGHTS

June 2022

Contributors

Cambridge Pro Bono Project – Project Managers:

Holli Sargeant

PhD Candidate, Law, University of Cambridge

Rebecca Xu

LLM Candidate, University of Cambridge

Faculty Supervisor:

Dr Stephanie Palmer

Associate Professor, Faculty of Law, University of Cambridge

Cambridge Pro Bono Project – Executive Committee:

Matthew Psycharis

PhD Candidate, Law, University of Cambridge

Student Researchers:

Apoorva Satapathy

Dushyant Kishan Kaul

Eleanor Bird

Isabelle St-Hilaire

LLM Candidates, University of Cambridge

About the CPP

The Cambridge Pro Bono Project

This research report addresses the legal process of implementing UNCRC general comment No. 25 (2021) on children's rights in relation to the digital environment in the United Kingdom ('**the UK**').

This report has been authored by members of the Cambridge Pro Bono Project ('**CPP**'), an initiative run out of the Faculty of Law at the University of Cambridge. The CPP is established to provide independent academic research on legal issues of public importance by drawing on the expertise of the researchers who study and work at the Faculty.

This research report is provided to 5Rights so that it might inform their work in this area. However, it is not supplied on the basis of a client-practitioner relationship, or on some other client-advisor relationship. This document, and the CPP's communications with AOAV, are not given as legal advice. The CPP remains an independent academic team and reserves the right to collaborate with other groups or persons working in this area, and to supply its research findings to those persons or groups.

Methodology

The CPP investigated the issues and implementation of the UNCRC General Comment No. 25 in the UK. The report considers:

- Subject matter risks to children's rights in the digital environment,
- Current UK legislation and policy in relation to General Comment No. 25,
- Identifies gaps and recommendations to improve current protections,
- Considers changes governments and business can make to advance full compliance with the General Comment No. 25,
- Reviews how to report to the UNCRC.

Content within the Boxes are examples we have identified relevant to subject matter.

To produce the report, the CPP recruited a cohort of legal researchers, supervised by doctoral candidates at the University of Cambridge. Production of the final report was reviewed by a senior member of the faculty, an expert in UK public law.

1 Introduction

The development of modern technologies and the increasingly ubiquitous nature of the internet has created a new digital environment for a connected child. That environment has become a fundamental aspect of how they grow up and experience the world. Specific consideration of a child's rights and interests with respect to the digital environment is therefore necessary to meet effectively their wellbeing and development needs.

The United Nations Convention on the Rights of the Child ('**CRC'**), which is the principal international law instrument aimed at protecting children's rights, was adopted in a largely analogue world and thus did not explicitly address the opportunities, risks and challenges in promoting children's rights in the digital environment.[1] In this regard, the UNCRC general comment No. 25 (2021) on children's rights in relation to the digital environment ('**GC**') represents a profound development. It is the first time that the acknowledgement of children as right-holders in the digital environment has been formalised.[2] Children have a fundamental right to access the digital environment. As highlighted by the GC:

> The digital environment provides a unique opportunity for children to realize the right to access information. In that regard, information and communications media, including digital and online content, perform an important function. States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary for the purposes stipulated in article 13 of the Convention.[3]

Accordingly, the 196 States Parties to the CRC, including the UK, will now have to consider how to implement the rights enshrined in the CRC, in light of the unique opportunities for the realisation of child rights as well as the risks and challenges that arise in the digital environment.

[1] *Convention on the Rights of the Child 1989* (UNTS 1577) ('*CRC*').

[2] *General Comment No. 25 on Children's Rights in Relation to the Digital Environment 2021* (CRC/C/GC/25) ('*General Comment No. 25*'); *Explanatory Notes General Comment No. 25 on Children's Rights in Relation to the Digital Environment 2021*.

[3] *General Comment No. 25* (n 2) 9.

This report aims to identify a legal and policy roadmap to the realisation of the GC in the UK. It evaluates current UK legislation and strategies that are relevant to children's rights in the digital environment, identifying gaps in protection and recommending practical solutions to address these gaps. In particular, this report assesses the UK legal framework on children's rights in the digital environment in the following areas: education, violence against children and criminal exploitation, commercial advertising and marketing, and gaming. First, it assesses the various child rights opportunities and impacts that are created by digital participation in these areas, including harms. It then evaluates the operation and effectiveness of relevant legislation in each area and makes recommendations to plug identified gaps in protection. The report also considers how to improve the UK's reporting mechanisms in relation to the UNCRC.

While written in the context of the UK legal framework, this report also reaches conclusions on the law more generally and its findings in relation to child rights issues and tensions arising in the digital environment is broadly applicable across all jurisdictions from a practical and policy perspective. For example, a particular tension created by the modern digital environment which all governments must tackle is the balancing of a child's crucial right to access the digital environment and make full use of all its benefits, and their right to be adequately protected from coterminous harms. Indeed, as the report shows, ensuring meaningful access to the digital environment is vital in supporting children to realise the full range of their civil, political, cultural, economic and social rights across diverse aspects of their lives, ranging from education to leisure. Thus, this report demonstrates that any movement of practical legal or policy action aimed at reaching the standards set out in the GC must begin from a basis of digital inclusion and empowerment, rather than restriction.

2 Education

Children's education, like other aspects of their lives, unfolds in part in digital environments. EdTech refers to the technological tools used for educational purposes. The development of EdTech tools, and even more so their use in schools, engages several child rights, notably their right:

- to have their best interests considered,
- to non-discrimination (which requires ensuring equal access to EdTech by removing potential barriers arising from socio-economic background or special needs, and combatting bias and inappropriate uses of profiling),
- to life, survival, and development - which may be promoted, according to some, through monitoring and surveillance software, though this risks interfering with other key rights),
- to have their views respected and considered (which may require involving them in decisions relating to the use of EdTech in their schools),

- to access information, freedom of expression, freedom of thought, conscience and religion, freedom of association,
- to privacy and to identity,
- and, of course, to education, culture, leisure, and play.

Legislative instruments relevant to the governance of EdTech in the UK include the Education Act 1996, the UK GDPR and the Data Protection Act 2018, the Age Appropriate Design Code. These are complemented by several policy and strategy documents, including the Department for Education Data Protection Toolkit for Schools, the UK EdTech Strategy 2019, the Ethical Framework for AI in Education, and Child Rights Impact Assessment processes.

There remain gaps in the current frameworks applicable to EdTech. In particular, there remains a lack of clear guidance on the respective roles of EdTech companies and schools with respect to the protection of children's data when EdTech tools are rolled out in school settings, as well as shortcomings with respect to transparency and compliance with existing rules. The present report summarises and builds on previous recommendations for remedying these gaps and presents insights from field research on strategies for making the most of EdTech's potential.

2.1 Background

Educational technology, or EdTech, is "typically defined as the sector of technology dedicated to the development and application of tools for educational purposes."[4] EdTech tools promise to support and improve children's education by making high quality and diverse educational materials easily available, providing interactive modes of learning and immediate feedback, and adapting to children's individual needs. However, the use of EdTech products also comes with risks. This is because they require schools and EdTech companies to collect and process significant amounts of personal data regarding children and their learning journeys. This may threaten children's privacy, expose them to economic exploitation, to profiling and discrimination. This is particularly concerning given that children and their parents may have limited choice when it comes to using an EdTech product mandated by their school. In addition, not all EdTech products are created equal from a purely educational standpoint: their effectiveness in achieving educational goals ought to be assessed rigorously and in a standardised manner.

In light of this, it is crucial to have a robust and clear data protection framework applicable to EdTech and a strong procurement process for selecting products to be used in state schools. Clarifying the rules and building a more robust process for developing, vetting, and selecting EdTech products, particularly for use in schools and managing the data generated through their service, will help ensure that children in the UK benefit from technological developments without sacrificing other important rights.

(a) Key terms

There are several forms of education data.[5] These are explained below.

[4] Vanessa Cezarita Cordeiro, 'Educational Technology (EdTech) and Children's Right to Privacy', *Humanium* (15 June 2021) <https://www.humanium.org/en/educational-technology-edtech-and-childrens-right-to-privacy/>; Elsewhere, EdTech has been referred to as 'a study and ethical practice for facilitating learning and improving performance by creating, using and managing appropriate technological processes and resources. In other words, use of technology in form of products/apps/tools to enhance learning, pedagogy and instruction. It is not replacing any current practices, but it is the use of those tools to aid in the delivery of education.' EdTech Editorial Team, 'What Is EdTech?', *EdTechReview* (15 February 2013) <https://edtechreview.in/dictionary/119-what-is-edtech>.

[5] Digital Futures Commission, *Governance of Data for Children's Learning in UK Sate Schools* (June 2021) 9 <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/06/Governance-of-data-for-children-learning-Final.pdf>.

Administrative data

This refers to data relating to, for example, attendance, school meals, school trips and school marketing.

Data processed by safety technologies

This refers to data relating to, for example, the 'monitoring and filtering of children's internet searches and communications.'[6]

Safety technologies may prevent children from accessing harmful or inappropriate content or prevent them from communicating with certain individuals, such as adults or perhaps even children from outside the school. However, as discussed below, the need to ensure children's safety must be balanced against children's other needs and rights, such as their right to access information, explore and develop their identity, and exercise their freedom of expression.

This category also includes suicide prevention and mental health support tools, discussed further below.

There is a stark contrast between the push for a privacy literacy curriculum (teaching children about the value of privacy and seeking to equip them to protect it) and the intense use of children's personal data in schools, which may result in serious invasions of their privacy.[7]

Learning EdTech data

This data is associated with tools more closely related to the school's curriculum delivery and children's learning experience. There are four categories within Learning EdTech:[8]

- organisational platforms,
- teaching and learning tools,
- personalised tools,
- predictive tools.

[6] Ibid 10.
[7] Velislava Hillman, 'EdTech in Schools – a Threat to Data Privacy?', *Media@LSE* (27 May 2021) <https://blogs.lse.ac.uk/medialse/2021/05/27/edtech-in-schools-a-threat-to-data-privacy/>.
[8] Digital Futures Commission (n 5) 34.

While the DFC 2021 Report focuses exclusively on Learning EdTech, several of the gaps and recommendations identified concerning Learning EdTech may also be relevant to other forms of education data.

2.2 Digital participation and potential harm

Children's use of Learning EdTech often involves little choice. Meaningful access to education and participation in school requires engaging with the tools prescribed by the child's school. In practice, this limits how the child and their parent or guardian can manage the risks involved by using these tools.

Box 1: Potential EdTech digital harm – an example

A parent might monitor a child's use of social media and gaming services and place restrictions on the sites and applications the child uses, the people they interact with on these platforms, and the amount of time they spend on them. By contrast, any parental involvement in the choice of Learning EdTech platforms is likely to be more remote (it might occur, for example, through participation in parent councils).

There is a need to find a balance between accessing the benefits of Learning EdTech and protecting children against the risks involved. The consequences of opting out of a learning tool used by the child's school might be more serious than, for example, opting out of a particular gaming site or social media platform.

Learning EdTech involves collecting and using potentially large quantities of data concerning a child, and this data can potentially be quite sensitive. More clarity is needed regarding who is allowed to collect, access and use this data, for what purposes and under what conditions, and who is ultimately responsible for safeguarding it. In addition, there is a need to consider the potential impact of Learning EdTech on a child's future opportunities: data collected about the child, and notably, the academic results obtained by a child, could follow them for a long time. Steps must be taken to avoid profiling pupils and prevent paths from being blocked off for a child too early.

2.3 Child rights opportunities and impacts

This section provides an overview of potential interactions between EdTech and rights protected by the CRC.

(a) Non-discrimination

The CRC mandates that State Parties "respect and ensure the rights outlined in the [CRC] to each child within their jurisdiction **without discrimination of any kind**, irrespective of the child's or his or her parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or another status."[9] It further requires that State Parties "take all appropriate measures to **ensure that the child is protected against all forms of discrimination** or punishment based on the status, activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members". [10] In the same vein, the GC "requires that State Parties ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them."

To achieve these standards, the UK must take measures to overcome digital exclusion and provide safe and free or affordable access to digital technologies in various settings. This includes EdTech.

Equal access – Socio-economic background

Children across the UK should have equal access to EdTech. This may not always be the case, given socioeconomic disadvantage. EdTech is meant to be used at home. As a result, the child's access will depend on the availability of household devices and the internet connection.

Research reported by Ofcom suggests that only a small percentage of school-aged children in the UK lack internet access or have access only through a smartphone.[11] However, limited internet access is associated with financial precarity,[12] making these children vulnerable. It will be important to ensure that the use of EdTech in the education system does not leave these children further behind.

[9] *CRC* (n 1) art 2.
[10] Ibid art 2.
[11] Ofcom UK, *Children and Parents: Media Use and Attitudes Report 2020/21* (28 April 2021) 52 Page 11 reads "Our Technology Tracker 2021 research found that nearly all UK households with school-age children (between 4 and 18 years old) had internet access in the home (less than 1% did not have access at home). However, 4% of these only had mobile access (that is, via a smartphone, tethering or dongle/USB, but with no fixed broadband). This decreased to 2% of those with only smartphone access (no tethering); Children in the 'most financially vulnerable' households (MFV) were more likely than those in the 'least financially vulnerable' (LFV) households to have mobile-only access (5% vs. 2%), or smartphone-only internet access (3% vs. 1%)." (footnotes omitted). .
[12] Ibid.

In addition, making the most of EdTech, especially when used at home, will depend on the students' and their parents' digital literacy.[13] As some parents may have lower levels of digital literacy and fewer resources, it may be useful for schools to invest in the digital literacy of the pupils and their parents. This could take the form of workshops or online tutorials teaching parents about the EdTech tools used by the school.

Equal access – Adaptation and accommodation

Children with special needs, including physical and sensory disabilities, learning disabilities, or developmental challenges, should not be forgotten with the development of EdTech. In theory, the personalisation of digital learning tools is one significant selling point; this feature should ensure that tools are adapted to individual needs.[14]

Bias and profiling

Where algorithms and AI tools are developed using historical data, there is a well-known risk of perpetuating underlying patterns of bias and discrimination. Therefore, to the extent that Learning EdTech tools rely on algorithms and AI, it is important to pay close attention to eliminating biases to ensure that these tools do not perpetuate negative biases against some children.

In addition, EdTech tools should avoid profiling children. Profiling involves using automatic data processing to apply a 'profile', namely a set of data characterising a category of individuals, to a specific individual, usually to inform decisions concerning that individual or to analyse or predict their preferences, attitudes, and behaviours.[15] EdTech tools ought to avoid profiling children which could block off paths too early.

Box 2: Bias in EdTech – an example

[13] See, generally, United Nations High Commissioner for Refugees, 'How to Ensure Everyone Can Continue Learning amid the Coronavirus Situation', *UNHCR* (6 April 2020) <https://www.unhcr.org/getinvolved/teachingtools/5e787bea4/ensure-continue-learning-amid-coronavirus-situation.html>.

[14] As discussed below.

[15] 'The protection of individuals with regard to automatic processing of personal data in the context of profiling' defines a 'profile' as 'a set of data characterising a category of individuals that is intended to be applied to an individual', and 'profiling' as 'an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.' Council of Europe, *The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling - Recommendation CM/Rec(2010)13 and Explanatory Memorandum* (October 2011) <https://rm.coe.int/16807096c3>.

If a child struggles with mathematics in fifth grade, EdTech tools should not steer them away from STEM subjects at such an early stage by suggesting certain courses or career paths to the detriment of others. Instead, EdTech tools should be used to palliate the child's current weaknesses and help them achieve their full potential. However, there may be cases where steering children towards their strengths and building on them will be appropriate and beneficial (especially as children get closer to making choices regarding their further studies and careers).

Care must be taken to protect various avenues for children, avoid labelling them, and set them on single-track paths with no possibility of reaching certain destinations.

(b) Best interests of the child

The CRC ensures that in "all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the child's best interests shall be a primary consideration."[16] A child's best interests will only be maximised by balancing the benefits of Learning EdTech and its potential risks.

(c) Right to life, survival and development

The CRC recognises "that every child has the inherent right to life" and requires that State Parties "ensure to the maximum extent possible the survival and development of the child."[17] It is undeniable that education plays a crucial role in a child's development. Used responsibly, Learning EdTech can positively contribute to child development. However, we should bear in mind that human interactions are also crucial to development; therefore, Learning EdTech should not replace or unduly interfere with interactions between teachers and children and amongst children.

There is an argument that EdTech can be used to help prevent suicides in children, in this way, it contributes to protecting their right to life and survival. EdTech tools may also have a role to play in preventing bullying. However, these functions must be balanced against this software's limits on other rights.

Box 3: Impacts on the right to life and development through EdTech

[16] *CRC* (n 1) art 3.
[17] *Ibid art 6.*

Dr Velislava Hillman, an expert in educational technologies, reveals concerns about EdTech.[18] Gaggle is a service used to prevent suicides by scanning students' coursework and behaviour for signs of depression; it comes pre-installed on Google Chromebooks used by students in some US schools.[19] While the service bolsters educators' and school administrators' confidence in their ability to monitor their students' mental health and intervene in time, if needed, this seems to come at a high cost to students' privacy.

However, issues with accuracy or bias from this service could have significant consequences. For example, suppose a student is flagged as a 'false positive' where they are predicted as suicidal or high-risk but are not, or the system indicates a 'false negative', and misses a student. In that case, they have differing but significant impacts. In particular, where EdTech is informed by machine learning that learns from historical data, there is no guarantee of accuracy.

In a promotional video for Gaggle, Dr Matthew X. Joseph, Director of Curriculum, Instruction and Assessment, describes Gaggle as "powerful" and "invisible".[20] He suggests that the best technology is seamlessly integrated for protection.[21] However, while the idea of a powerful tool running smoothly in the background to protect children has an undeniable appeal, it should not mean that potentially harmful technology is absent from view. On the contrary, their strengths and weaknesses, merits, and implications for students' privacy should be openly and thoroughly evaluated, reflected upon, and debated.

(d) Respect for the views of the child

Children should be allowed to be involved in decisions relating to EdTech in their schools.[22] It is important to respect children's views concerning participation in the design choices and opportunities for deployment using EdTech.

Box 4: Participation in EdTech design

Student representatives could participate in the choice of EdTech platforms, the enabled features, and the default settings on such platforms. There could also be mechanisms to allow individual children and parents to challenge decisions relating to their use of EdTech, for example, by establishing a process by which they could bring their concerns or complaint to the teacher or a designated member of the school's administrative staff. These could be escalated to a special committee created by the school board to resolve difficult cases.

[18] Hillman (n 7).
[19] Gaggle Net Inc, 'Student Safety That Saves Lives' <https://www.gaggle.net>.
[20] Ibid.
[21] Ibid.
[22] *CRC* (n 1) art 12.

(e) Civil rights and freedoms

Access to information

The child's right to access information is crucial as it is a precursor to exercising several other rights. As children develop, they cannot build their sense of identity, develop their thoughts and beliefs, or properly express themselves, if they do not have access to information.[23] EdTech can be used to facilitate access to information by providing age-appropriate, digestible materials on a variety of topics of interest to students.

How the information is curated on these platforms deserves attention: while choices must inevitably be made, and some material may be deliberately excluded on the basis that it would be harmful (overly violent content or content containing discriminatory messages, for example), it is important to expose children to a variety of viewpoints and to allow them to exercise agency for the information they access and the topics they learn.

[23] 'Ensuring children have access to information from a variety of sources is key to helping them make up their own minds about what they think and how they express themselves', see e.g., Child Rights International Network, 'Article 13: Freedom of Expression' <article-13-freedom-expression.html>.

Restrictions on children's use of search engines at school are particularly difficult to assess from a rights perspective. Again, while some restrictions will be justifiable and necessary, they should be tailored meticulously and reviewed frequently. Students should not be indiscriminately barred from accessing sensitive information on sexual health, controversial political opinions, world conflicts or other tragedies. Rather, limits should reflect the age of the children, the degree of harm associated with the content (for example, how extreme or graphic a particular piece of content is). Instead of being completely shielded from difficult topics, they should be discussed in class in such a way that children can be guided through them in an age appropriate manner. The curriculum on digital literacy for older children could incorporate a discussion of these restrictions to foster critical thinking in their pupils. Parents and older students could be made aware of such restrictions to enable a public debate about how to tweak them – parents and students could challenge restrictions they view as overly strict or suggest that others be added when a gap is identified. One might think of sensitive topics such as the role of immigration in building society,[24] and sexual health and well-being,[25] where input from parents, students and experts may play an important role in determining what type of content should be included or excluded on EdTech platforms.

Concerning the monitoring of a child's searches, it is important to reflect on the impact that this may have on children's ability to access information: the feeling of being observed, or being pulled aside to discuss unusual search patterns, may have a chilling effect on children's willingness to explore personal or sensitive topics of interest.

[24] By way of example, an assignment found in a 2011 Canadian textbook asking students to debate immigration policy has been criticized for offering anti-immigration arguments, which community members identified as racist, xenophobic, and liable to making racialized and/or immigrant students feel unwelcomed and singled-out. Commenting on the assignment , the Minister of Education acknowledged the importance of encouraging critical thinking while highlighting the need to approach the material 'with sensitivity and respect'; he also noted the department was ' 'looking at removing the textbook from the curriculum'. See Meg Roberts, '"Racist" Junior High Immigration Assignment Has Advocates Calling for Curriculum Change | CBC News', *CBC News* (online, 17 January 2022) <https://www.cbc.ca/news/canada/newfoundland-labrador/immigration-assigment-textbook-1.6315301>.

[25] In some communities, the appropriate breadth of the sexual health curriculum to be delivered in schools is a highly contested issue. For example, one Alaskan school district recently grappled with whether informative videos prepared by Dr. Danielle Jones, a board-certified obstetrician and gynecologist and popular YouTuber, could be added to list of approved supplemental sex ed materials. See Dermot Cole, 'Fairbanks School Board Stumbles on Sex Ed, Doctor's YouTube Responses Draw 1 Million-plus Views', *Reporting From Alaska* (online, 3 January 2022) <https://www.dermotcole.com/reportingfromalaska/2021/12/27/a3k5pkf16ui8xzyqpmiz9f6q67pvtt>.

Freedom of expression

The CRC recognises the child's right to express their ideas through the media of their choice.[26] As noted in the GC on the aims of education, this includes expressing their views on the content of the curriculum as well as the educational process, the teaching methods, and the educational environment more broadly.[27]

EdTech tools can help children express themselves through digital means.

Box 5: Freedom of expression in EdTech

As an example, messaging tools, language learning platforms, spelling games, and storytelling games may support children's development and exercise of expressive skills. Therefore, they could conceivably be considered EdTech tools or be integrated into such tools. Common Sense Media reviews apps and games, among other media that may interest children.[28] Recommended media featured on their website include, for example, TalkingPoints and Klassly for school-to-home communication and Kinzoo and Azoomee communication within families; Duolingo and Drops for language-learning; Lexi's World for spelling; and Rory's Story Cubes, Toontastic 3D, and Book Creator for storytelling.[29] While other analogue techniques such as visual plastic art should not be ruled out, becoming comfortable with digital modes of expression will help children communicate their ideas, feelings and needs in the digital world.

[26] *CRC* (n 1) art 13.
[27] *General Comment No. 1 Article 29 (1) on the Aims of Education 2001*; Child Rights International Network (n 23).
[28] Common Sense Media, 'Common Sense Media: Age-Based Media Reviews for Families' <https://www.commonsensemedia.org/> ('*Common Sense Media*') Common Sense Media receives funding from several foundation partners, including the Chan Zuckerburg Initiative, The Bill and Melinda Gates Foundation, The Bezos Family Foundation, Twitter, to name a few.
[29] Ibid Common Sense Media receives funding from several foundation partners, including the Chan Zuckerburg Initiative, The Bill and Melinda Gates Foundation, The Bezos Family Foundation, Twitter, to name a few.

Freedom of expression comes with responsibilities. Article 13 of the CRC acknowledges that the right to freedom of expression may be subject to certain restrictions if necessary and provided by law, notably to ensure "respect of the rights or reputation of others".[30] Children should be taught about the consequences of their expression: how their words matter, how they can be used for change but can also hurt others, and how it can be difficult to take them back.[31] As the Child Rights International Network points out, exercising their freedom of expression to voice their feelings and opinions enables children "to describe how their rights are respected or infringed and learn to stand up for the rights of others".[32]

In light of this, we suggest that EdTech tools should be designed to foster expression. This should be done to allow children to maintain some control over their expression, now and in the future. By default, a student's expressive work should remain private or at least within the school's boundaries and published only after careful consideration and with the student's consent. In addition, children should receive guidance on the potential consequences of putting their thoughts and opinions "out there" – this should be part of the digital literacy curriculum. Finally, as discussed in the section on social media, youth are increasingly involved in sharing aspects of their lives, thoughts, and opinions online. While this may support the exercise of their freedom of expression, they are entitled to learn about the risks associated with such public sharing.

Freedom of thought, conscience and religion

The CRC requires that State Parties "respect the right of the child to freedom of thought, conscience and religion."[33] Education material contributes to shaping a child's thoughts and beliefs. Where schools deliver a religious curriculum, the educational system is also involved in the child's religious upbringing; to a lesser extent, teaching about world religions may also support the child's right to freedom of religion. EdTech tools should foster freedom of thought, belief and religion, which can be accomplished by promoting the related rights of access to information and freedom of expression. This means ensuring that children could be exposed to various opinions and are given the tools and space to formulate and share their own opinions. To achieve this, we must pay attention to and carefully select the content available on EdTech platforms, choose tools that foster critical thinking and leave plenty of space for interaction among students and teachers.

[30] *CRC* (n 1) Art 13(2)(a).
[31] This can be incorporated with strategies for preventing bullying.
[32] Child Rights International Network (n 23) 13.
[33] *CRC* (n 1) art 14.

Freedom of association and peaceful assembly

It is interesting to consider how EdTech platforms may facilitate or hinder student organisations and movements. While safety always remains an important consideration, EdTech tools should support children's right to freedom of association and peaceful assembly. This could mean that students are allowed to use messaging features on platforms used at their school to communicate with one another, arrange meetings and organise themselves without interference from teachers or school administrators – or, at the very least, that they are not blocked from doing so on messaging platforms other than the EdTech platforms used by the school.

Schools might at times be tempted to manage student activism. Still, it should be kept in mind that student organisations and associations are important to developing a healthy democracy by raising children who become attentive and involved citizens.

Right to privacy

As with all forms of digital participation involving children, ensuring that EdTech tools are developed and used to respect children's right to privacy is axiomatic. As mentioned, EdTech tools may involve collecting, generating and processing significant amounts of personal data, often of a sensitive kind. In addition to demographic details, EdTech tools may record academic achievements and results on even the most informal tests, exercises and homework, as well as content – such as journal entries prepared as part of a written assignment – reflecting the child's emotional state, their concerns, worries, fears, hopes and dreams. Other assignments may reflect their developing political and world views and aspects of their emerging sense of identity. EdTech tools of an administrative nature might, in theory, collect information on a child's absences, incidents when they got into trouble, aspects of their medical history, consultations with a guidance counsellor, school nurse or school psychiatrist, right down to a list of their bathroom breaks.

Box 6: Right to privacy in EdTech

For example, software called e-Hallpass is used in some schools in the US. It requires students to request permission for a bathroom break on their school-issued computer or personal smartphone, which a teacher then approves "pending any red flags in the system, such as another student he should avoid out in the hall at the same time".[34] Should the student be "out of class for more than a set amount of time, the application would summon an administrator to check on [them]".[35] The company that makes e-Hallpass, Eduspire Solutions, indicates that the "system is meant to keep track of students in an emergency, decrease vaping, identify vandals and crackdown on truancy". Eduspire Solutions suggests that it collects the same information that schools used to collect on paper while providing a more sanitary alternative to germ-covered physical objects previously used as hall passes.[36] It also highlights that schools control the data and choose how often to delete it. However, some students have decried the use of the software as invasive and as violating their privacy and have signed a petition to have it removed from their school.[37] Similarly, privacy attorney Brad Shear, a parent to two elementary-age children, refers to this app as 'bathroom big brother' and vows he will not allow it to be used in his children's schools.[38]

Given the extent to which the use of EdTech in schools can contribute to painting a detailed digital portrait of a developing child, it is crucial to take steps to protect their right to privacy concerning this wealth of personal information. We should also carefully reflect on whether all of this information needs to be recorded digitally, whether it can be quickly erased, and with whom it should be shared.

[34] Heather Kelly, 'School Apps Track Students from Classroom to Bathroom, and Parents Are Struggling to Keep Up', *Washington Post* (online, 29 October 2019) <https://www.washingtonpost.com/technology/2019/10/29/school-apps-track-students-classroom-bathroom-parents-are-struggling-keep-up/>; See also Shubham Sharma, 'Now, US Schools Use App to Track Kids' Bathroom Breaks', *NewsBytes* (5 November 2019) <https://www.newsbytesapp.com/news/science/school-using-app-to-track-kids-bathroom-breaks/story>.

[35] Kelly (n 34); See also Sharma (n 34).

[36] Kelly (n 34); See also Sharma (n 34).

[37] Kelly (n 34); See also Sharma (n 34).

[38] Kelly (n 34); See also Sharma (n 34).

Right to identity

EdTech tools should foster the identity formation process rather than hinder it. This can be achieved by protecting the right to identity and the associated rights with which it interacts. As children develop, they build their identity, and it is undeniable that childhood and teenagerhood are crucial periods for this process. Moreover, school is one of the key venues children forge their identity, and education is an essential contributor to identity formation. The right to identity interacts with access to information, freedom of expression, freedom of thought, belief and religion, freedom of association, and privacy. Indeed, the child needs to access information and cultural material to acquire the building blocks from which they will construct their identity – this may be particularly true of the ethnic, cultural, linguistic, sexual and gender aspects of their identity. A limited or restrictive curriculum risks 'restrict[ing] children's civil and political rights and legitimise discrimination.'[39] By way of example, the Child Rights International Network points to the finding reached in 2007 by the European Committee of Social Rights, responsible for monitoring States' compliance with the European Social Charter, 'that Croatia's limited curriculum on sex education discriminated against the basis of sexual orientation'.[40]

As part of exercising their right to identity, children need to be free to think about themselves and the world, interact and gather with others with whom they identify, and express their fluid identity. The child also needs a private space to develop their sense of identity, to iterate 'draft' identities that they will then test out in the real world. EdTech tools must be designed to respect and protect that private space and support the process of identity formation.

2.4 Education, leisure and cultural activities

(a) Right to education

It goes without saying that EdTech is relevant to a child's right to education.[41] We must ensure that EdTech fosters a better education for all UK children, rather than decreasing the quality of their education. The promise of EdTech lies in increasing the breadth of resources available to children, but more importantly, in personalising curriculum delivery, for example, by tailoring it to a child's specific needs. So, for example, quizzes delivered on an EdTech platform could quickly identify that a student is struggling with a concept, prompting them to review the lesson explaining that concept and repeat relevant exercises to help them assimilate the concept and improve their skill.

[39] Child Rights International Network (n 23) 13.
[40] Child Rights International Network (n 23).
[41] *CRC* (n 1) art 28, 29.

Box 7: Education and YouTube kids

A report on YouTube Kids found that only 5% of the videos shown had educational value, and only 24% showcased diverse representations of race and gender. In addition, the inappropriate content shown to children does not promote their social or mental health. Instead, children are not presented with adequate material. YouTube Kids content neither promotes the diversity of cultural and international sources nor encourages the production and dissemination of children's education.[42]

Child-directed YouTube videos have also been noted to have high levels of commercialism. In addition, Although YouTube Kids was released in 2015 to provide a site for children to watch YouTube content without the data collection or behavioural advertising practices on the main YouTube platform, young children continue to use YouTube often, in some studies, more frequently than YouTube Kids.[43]

(b) Right to culture leisure and play

Education is closely linked with culture.[44] Learning EdTech could facilitate access to cultural material, expose children to various cultures, and foster each child's relationship with their own culture. In addition, Learning EdTech can integrate play, making learning fun and interactive. However, Learning EdTech should not monopolise the space for play in the education context: children should continue to enjoy "pure" leisure time (exempt from any pressure or expectation of pursuing learning objectives) as well as time for interacting with friends in classmates in person, free from digital distractions.

[42] Common Sense Media, *Young Kids and YouTube: How Ads, Toys, and Games Dominate Viewing* (2020) <https://www.commonsensemedia.org/sites/default/files/research/report/2020_youngkidsyoutube-report_final-release_forweb.pdf>.
[43] Ibid.
[44] ibid art 31.

2.5 Protections

(a) Protection from violence, abuse and neglect

There is a debate regarding whether, or under what circumstances or under what conditions, software incorporated into EdTech tools should be used to detect patterns of violence, abuse, and neglect involving a pupil. As with the discussion on the right to life and survival, the possibility of detecting a risk of harm or a current harmful situation and intervening to protect the child must be weighed against the privacy costs and the damage that could result from wrongly identifying a child as being at risk of violence, abuse or neglect. As emphasised in a news article about the use of artificial intelligence (AI) in the UK's child safeguarding system by combining "vast amounts of data from a variety of sources", in addition to questions about whether such techniques outperform traditional analysis, "the other issue for wider debate is whether politicians and the public are comfortable with the harvesting of personal data in this way – even if it does offer the prospect of saving a child's life".[45]

In particular, machine learning in social care may lead to the "unethical profiling of groups of people."[46] For example, disadvantaged, racialised families tend to suffer disproportionately from being wrongly targeted by artificial intelligence (AI) tools designed to identify at-risk children. Thus, if used at all, AI incorporated in EdTech tools as elsewhere should be "only part of the process", with "[f]urther verification and checks [being] carried out in line with statutory requirements before any intervention", representing "merely another piece of the toolkit to aid decision-making."[47]

As mentioned above in the section on access to information, it is also worth reflecting on the extent to which EdTech should protect children from being exposed to violent content. We posit that the parameters and content available through EdTech should be tailored to the children's age and maturity and the context of the topics discussed in class. While children should not be exposed to extremism or extremely violent games at school, they should not necessarily be shielded from every topic that could be viewed as associated with violence. Discussion of historical and current events, such as wars and conflicts, and difficult but important issues like domestic violence, can be surfaced in an age-appropriate and sensitive manner. EdTech tools can assist with this, but face-to-face interactions will likely remain important in discussing sensitive topics with developing minds.

[45] Lynn Eaton, 'Is It Right to Use AI to Identify Children at Risk of Harm?', *The Guardian* (18 November 2019) <https://www.theguardian.com/society/2019/nov/18/child-protection-ai-predict-prevent-risks>.
[46] Ibid.
[47] Ibid.

EdTech should certainly protect children from predators. This threat should be relatively easy to manage in education compared to social media or gaming. An EdTech platform tends to be a much more controlled environment, often created specifically and perhaps exclusively for children. The risk posed by teachers/educators with malign intentions, while small, should not be ignored. Indeed, a legitimate query arises about whether the use of EdTech tools providing teachers with increased access to a child's data and heightened control (or perceived control) over the child's future might sharpen the power dynamics between a predatory teacher and a vulnerable child.

(b) Protection from economic, sexual and other forms of exploitation

Some uses of data by EdTech companies might be seen as exploitative. Tech companies thrive on data, almost using it as a raw material. To what extent should children's data be used to quench this insatiable thirst? It must be understood, of course, that EdTech companies must use some data to perform services and that some analyses relying on large data samples may assist them in developing improved tools and detecting biases. Nevertheless, determining who accesses what data, under what conditions, and for what purposes are important conversations to have to ensure that children's data are not improperly used or exploited.

Furthermore, it will be important to consider what kinds of relationships EdTech should be allowed to entertain directly with parents and pupils. Where EdTech companies contract with schools or school districts to dispense certain services, in what circumstances should they be allowed to sell additional services or features to parents above what is provided through the school? When would such practices be considered exploitative? Parents may feel pressured to pay for access to additional services offered by the EdTech company, whose products are already integrated into their child's education. They may fear that refusing to pay for such access could place their child at a disadvantage. Of course, parents are always free to purchase additional resources to support their child's education – from additional books to private tutoring – but the idea of selling products as add-ons seamlessly integrated with the platform the child uses at school seems to take things to a different level. While some may give important weight to contractual freedom, it is worth considering how to prevent the practices of EdTech companies from taking on exploitative colours.

2.6 General measures of implementation by the United Kingdom

(a) Legislation

Education Act 1996

Schools must collect data from children in state schools each term (**National School Data**), including allocating a Unique Pupil Number (**UPN**) to each student when they first enrol in a state school[48] and provide such information to the Department for Education (**DfE**).[49] Information collected by schools should be anonymised to not be connected to the name of any pupil.[50] In particular, information should not be published in any form which includes the name of the pupil to which it relates.[51] Some provisions concern the sharing of individual pupil information between different government departments or with other bodies responsible for collating information relating to pupils in connection with the Secretary of State relating to education.[52]

Schools are also mandated to assign each student a Unique Learning Number (**ULN**), used as an identifier for their Personal Learning Record. Students' Personal Learning Records contain data that schools can transfer to other schools attended by the child.[53]

Data Protection Framework

Access to National School Data by researchers and private companies in EdTech must comply with the Data Protection Act 2018 (**DPA**), the UK implementation of the General Data Protection Regulation (**GDPR**) and the Privacy and Electronic Communications Regulations 2003 (**PECR**).[54]

[48] *Education Act 1996* ss 537, 537A.
[49] Digital Futures Commission (n 5) 12.
[50] *Education Act 1996* (n 48) s 537(5).
[51] Ibid s 537A(7).
[52] Ibid s 537A.
[53] Ibid s 408; Digital Futures Commission (n 5) 12.
[54] Digital Futures Commission (n 5) 12.

Data controllers must carry out a data protection impact assessment (**DPIA**) when "processing is likely to result in a high risk to the rights and freedoms of individuals".[55] The ICO defines the DPIA as a process aimed at helping to identify and minimise the data protection risks of a project.[56] When EdTech projects are being developed, DPIAs should be carried out.[57] The AADC advises entities to undertake a DPAI to assess and mitigate the risk to children's rights and freedoms likely to access their service. Further, this DPIA process should consider the differing ages, capacities, and development needs and ensure that the DPIA builds in compliance with the AADC.[58] Indeed, EdTech projects are likely to be "major project[s] involving the use of personal data" and often involve several elements that make DPIAs more likely to be warranted or required, such as evaluation or scoring, systematic monitoring, processing data of a highly personal nature, processing on a large scale, processing of data concerning vulnerable data subjects, innovative technological or organisational solutions, process children's personal data for profiling or automated decision-making or marketing purposes, or offer online services directly to them.[59]

Box 8: Conducting a DPIA for EdTech

The steps involved in a DPIA can be summarized as (1) identifying the need for a DPIA, (2) describing the processing, (3) considering consultation, (4) assessing necessity and proportionality, (5) identifying and assessing risks arising from the processing, (6) identifying measures to mitigate the risks, and finally (7) signing off, recording and integrating outcomes.[60]

[55] *Data Protection Act 2018* s 64; *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016* (OJ 2016 L 119/1) ('*GDPR*') s 34.

[56] Information Commissioner's Office, 'Data Protection Impact Assessments' (28 February 2022) <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/>.

[57] Digital Futures Commission (n 5) 19.

[58] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* (2020) 26 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>.

[59] Information Commissioner's Office, *Data Protection Impact Assessments* (n 56).

[60] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 26.

As mentioned, conducting a DPIA is the responsibility of the data controller. However, as discussed further below, it may not always be clear who, between the EdTech provider and the school, is the data controller or whether they are joint controllers. In our view, in any event, it would be preferable for both the EdTech provider *and* the school (or school district) to be involved in assessing the data protection impacts of the project, either by each conducting their own or DPIA or by conducting a joint DPIA (as if they were joint controllers). This is because they can contribute different perspectives and information to the exercise: EdTech companies have more in-depth knowledge of what data their products collect and what could and is intended to be done with that data, while schools are likely (one might hope) to be more attuned to the effects that data collection and use may have on pupils.

AADC

The Age Appropriate Design Code (**AADC**) is a statutory code of practice[61] that "applies to 'information society services likely to be accessed by children' in the UK", including, *among other things*, "news or educational websites".[62] Thus, in our view, the AADC ought to apply to EdTech products: they are information society services (i.e., digital, informational services) not only *likely* to be accessed by children but *expressly designed and marketed* for children. Indeed, as an example of data sharing that might occur routinely, the AADC points to "the provider of an educational app routinely sharing data with the child's school".[63] However, as discussed below, there are conflicting views in the literature as to whether EdTech providers and schools are compelled to abide by the AADC. The uncertainty and debate on this point risk making the AADC less effective in ensuring that EdTech tools are, by design, respectful of children's rights, resulting in a gap in the current framework, also discussed below.

[61] Prepared under s 123 of the *Data Protection Act 2018* (n 55).
[62] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 14–15.
[63] Ibid 55.

(b) Comprehensive policy and strategy

Department for Education Data Protection Toolkit for Schools

The DfE toolkit was published as an 'open beta' document or 'living' document. The toolkit aims to support schools in adapting their data protection and privacy practices to comply with legislative changes brought by the GDPR and DPA in light of the school's particular use of data and related technologies.[64] The document describes nine steps to "help schools efficiently develop the culture, processes and documentation required to be compliant with the strengthened legislation and effectively manage the risks associated with data management."[65] However, the toolkit warns that it provides tips and guidance only, not formal legal advice, and that "as a data controller in its own right, a school is ultimately responsible for its data protection procedures and compliance with legislation."[66]

The nine steps are the following: (1) raising awareness, (2) creating a high-level data map, (3) turning the data map into a data asset register, (4) documenting the reasons for processing the data, (5) documenting how long the information needs to be retained for, (6) identifying and mitigating risks that emerge from the initial completion of the data asset register, (7) deciding on the Data Protection Officer role, (8) communicating with data subjects, and finally (9) operationalising data protection and keeping it living.

UK EdTech Strategy 2019

In 2019, the Department of Education published a strategy document titled *Realising the potential of technology in education: a strategy for education providers and the industry*. Aside from setting out a vision for education technology – one that sees EdTech not as a silver bullet but as a 'thread woven throughout the processes of learning and teaching' and that focuses on determining how it can best support these processes – the strategy contains sections on promoting digital safety as well as supporting effective procurement and developing a dynamic EdTech business sector. These objectives may sometimes come into tension with each other. The strategy acknowledges that:

[64] Department for Education, *Data Protection: A Toolkit for Schools* (31 August 2018) 7 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf>.
[65] Ibid.
[66] Ibid.

> Many are rightly concerned about the privacy, security and safety implications that come with adopting technology. Education leaders and teachers will have seen the problems that can come with poor products and poor implementation. Information and cyber security are fundamentally about understanding and acknowledging risks and working through all avenues to appropriately reduce them.[67]

The strategy thus highlights that:

> EdTech suppliers should adhere to the Cyber Essentials minimum standards developed by the National Cyber Security Centre as well as the guidelines developed within the government's Code of Practice for Consumer IoT Security to ensure that any products connected to the internet are secure by design.[68]

However, while this addresses privacy and security-related harms, it does not engage with the full range of children's rights affected by the expansion of the EdTech sector and the use of EdTech in schools.

[67] Department for Education, *Realising the Potential of Technology in Education: A Strategy for Education Providers and the Technology Industry* (2019) <https://www.gov.uk/government/publications/realising-the-potential-of-technology-in-education> ('*EdTech Strategy*').
[68] Ibid.

Child Rights Impact Assessment process

Generally speaking, a Child Rights Impact Assessment (**CRIA**) is "a tool predicting the impact of any proposed law, policy or budgetary allocation, which affects children and the enjoyment of their rights."[69] It is described as an 'iterative process' used to evaluate the effects of legislative or policy proposals both before and after they are implemented, examining their intended and actual consequences on children, and allowing for course-correcting adjustments to be made throughout the process.[70] The impetus for CRIAs derives from States' role as primary duty-bearers for protecting human rights and for public decision-makers; however, a similar rationale has been extended to businesses.[71] CRIAs can and should be applied to digital services geared at children. In fact, it has been recommended that a CRIA be carried out on EdTech products, in addition to a DPIA, before selecting them for use on a national scale.[72] Indeed, it would be beneficial for EdTech companies to carry out CRIAs as they develop their products. In addition, unless and until a national selection and roll-out program is developed for procuring EdTech products, schools or school districts should carry out CRIAs themselves.

[69] FRA, 'Child Rights Impact Assessment', *European Union Agency for Fundamental Rights* (24 November 2014) <https://fra.europa.eu/en/content/child-rights-impact-assessment>.
[70] Sonia Livingstone, Sudeshna Mukherjee and Kruakae Pothong, *Child Rights Impact Assessment: A Tool to Realise Children's Rights in the Digital Environment* (March 2021) 38 <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf>.
[71] Ibid 13.
[72] Ibid 38.

While CRIAs ought to help ensure respect for the rights set out in the UNCRC, and while the UK Government has committed itself to give due consideration to the UNCRC Articles when developing new legislation and policy,[73] conducting a CRIA is not a legal requirement per se applicable throughout the United Kingdom. This may be contrasted with the Equality Impact Assessment, defined as a systematic and evidence-based tool that enables consideration of the likely impact of an initiative on different groups of people, the completion of which is 'a legal requirement under race, disability, and gender equality legislation'.[74] It is also interesting to note that the Northern Ireland Executive has adopted a national approach, known as the Children and Young people's Strategy 2020-2030, 'to systematically consider children's rights, as part of its mandatory EQIA', thus integrating an inescapable child-rights perspective into the legal-required EQIA.[75] It is also interesting to note that the Council of Europe has issued a Recommendation on the rights of the child in the digital environment calling on States to conduct CRIAs, as well as to require businesses to assess the risks of their products.

It may be advisable to make separate CRIAs legally required throughout the United Kingdom or make CRIAs an obligatory part of the legally required EQIAs. In the meantime, EdTech providers and schools or school districts should be encouraged to conduct CRIAs, notwithstanding their lack of a legal mandate.

Ethical Framework for AI in Education

In addition to conducting DPIAs and CRIAs, it has been suggested that "[l]earning EdTech that use algorithms should evidence compliance with standards related to the use of AI, such as the Ethical Framework for AI in Education"[76] developed by the Institute for Ethical AI in Education.[77]

[73] Lisa Payne, *Child Rights Impact Assessment (CRIA): A Review of Comparative Practice across the UK* (UNICEF UK, 2017) <https://www.unicef.org.uk/wp-content/uploads/2017/09/Unicef-UK-CRIA-comparative-review_FOR-PUBLICATION.pdf>.
[74] Livingstone, Mukherjee and Pothong (n 70) 30.
[75] Ibid 19.
[76] Digital Futures Commission (n 5) 40.
[77] The Institute for Ethical AI in Education, *The Ethical Framework for AI in Education* (Final Report, March 2021) <https://www.buckingham.ac.uk/research-the-institute-for-ethical-ai-in-education/>.

The framework comprises a list of objectives, criteria, and a checklist for evaluating whether each is achieved. These objectives are: (1) achieving educational goals; (2) forms of assessment ("AI should be used to assess and recognise a broader range of learners' talents"); (3) administration and workload "AI should increase the capacity of organisations whilst respecting human relationships"; (4) equity; (5) autonomy; (6) privacy; (7) transparency and accountability; (8) informed participation ("[l]earners, educations and other relevant practitioners should have a reasonable understanding of artificial intelligence and its implications"; (9) ethical design.[78] The framework thus presents concrete steps that can be taken to improve the overall quality and safety of EdTech products.

(c) Allocation of resources

Developing and implementing EdTech solutions can attract hefty costs and require the dedication of significant human resources. Therefore, it is important to consider whether it is worth diverting resources away from other types of initiatives within the education sphere – in other words, whether the payoffs will be worth the costs or whether resources would be better spent elsewhere. This is particularly so where funding is scarce: "unused education technology can be an unnecessary expenditure for cash-strapped education systems".[79] For example, will adding electronic whiteboards to classrooms facilitate access to more quality content or differentiated instruction? Or will these expensive boards be used the same way as the old chalkboards? Will providing one device (laptop or tablet) to each learner facilitate access to more and better content or offer students more opportunities to practice and learn? [80]

Further, they warn that:

> Solely introducing technology in classrooms without additional changes is unlikely to improve learning and may be quite costly. Suppose you cannot identify how the interactions among the three key components of the instructional core (educators, learners, and content) may change after introducing technology. In that case, it is probably not a good idea to invest.[81]

[78] Ibid 5–9.
[79] Alejandro Ganimian, Emiliana Vegas and Frederick Hess, 'Realizing the Promise: How Can Education Technology Improve Learning for All?', *Brookings Institute* (10 September 2020) <https://www.brookings.edu/essay/realizing-the-promise-how-can-education-technology-improve-learning-for-all/> ('Realizing the Promise').
[80] Ibid.
[81] Ibid.

Even – and perhaps especially – when allocating resources to EdTech, it is also crucial to think about distributional issues. As the World Bank notes, '[t]oday, the use of EdTech has demonstrated and is exacerbating inequities in education systems', but '[t]his need not be the case'.[82] The greatest potential for the use of technology in education is to level the playing field among students and ensure equal opportunities are afforded to them.[83] By thinking carefully about where and how technology might have the greatest impact (and implementing strategies discussed further below), administrators may harness EdTech to help bridge educational gaps between socioeconomic groups and, ideally, improve learning outcomes for all pupils.

2.7 Gaps in current frameworks

The present section explores potential gaps in the current legislation and frameworks governing EdTech.

(a) Lawful processing of data

Previous research has revealed the existence of some confusion on how the UK GDPR and the DPA 2018 should apply to education data processed by EdTech companies.[84] There is a lack of clarity regarding who the data controller and data processors are in different EdTech scenarios – it is difficult to identify who the data controller is between the school and the EdTech company.[85] Yet correctly identifying who wears which hat is important because an organisation's obligations under the UK GDPR vary depending on whether they are a controller, a joint controller, or a processor.[86] Indeed, data controllers bear more responsibility for ensuring respect for data protection laws. They are the 'main decision-makers, determining how and what data will be collected and used. In the form of checklists, the ICO guides organisations on determining whether they are a controller, a joint controller, or a processor.[87]

[82] 'Education and Technology', *World Bank* <https://www.worldbank.org/en/topic/edutech>.
[83] {Citation}
[84] Digital Futures Commission (n 5) 24.
[85] Ibid.
[86] Information Commissioner's Office, 'Controllers and Processors' (1 January 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/>.
[87] Ibid.

There is disagreement on whether children can enter a contract in an educational setting. EdTech companies often rely on a contract as a lawful basis for controlling and processing children's data for non-core purposes relating to optional features that children can opt-in to. However, it has been argued that children cannot enter a contract in an education setting.[88] In our view, a contract is an inappropriate basis to ground the lawfulness of processing pupil's personal data by EdTech companies in an educational setting. This is for two main reasons. First, it is unrealistic for children to understand the intricacies of the contract provisions. Second, the power imbalance between the child and the EdTech company is too great to make a contractual agreement meaningful and truly voluntary, not only because of the child's previous limited understanding of contractual terms, their limited maturity and their vulnerability, but also simply because children are likely to be under excessive pressure to acquiesce to contractual terms when this is required to use the features of a platform that are recommended by their teacher and/or used by their peers.

Lack of transparency is another recurring theme in previous research conducted by 5Rights. The DFC 2021 recommends that "Learning EdTech companies should be required to publish their legitimate interests assessments when using this legal basis".[89] More generally, perhaps EdTech companies should be required to publish their DPIA and CRIA,[90] or at least to provide it to an authoritative body, perhaps the ICO.

(b) Profiling

As research conducted by 5Rights previously noted, Article 22 of the UK GDPR limits the profiling of children, providing that decisions that have legal or similarly significant impacts on a person (including a child) should not be made solely by automated processing of their data, unless one of three exemptions applies, namely that:

'It is necessary for the performance of a contract between the Learning EdTech company and the child, and the company has put in place suitable measures to safeguard the child's rights, freedoms and legitimate interests;

It is authorised by UK law, which includes suitable measures to safeguard the child's rights, freedoms and legitimate interests;

It is based on the child's explicit consent, and the company has put in place suitable measures to safeguard the child's rights, freedoms and legitimate interests.'[91]

[88] Digital Futures Commission (n 5) 24.
[89] Ibid 41.
[90] Ibid 34.
[91] Ibid.

Thus, safeguards of one form or another must always be in a place where decisions concerning children are made solely based on automated processing. We would add that safeguards and careful consideration should be applied even when the automated processing forms only part of the decision-making process. In such circumstances, the profiling of children could still seep into the ultimate decision of the human decision-maker; therefore, care must be taken to avoid bias being incorporated into the automated processing step.

Furthermore, profiling a child should only be permitted to improve the educational services provided to that child and cater to their learning and development needs. To the extent that profiling is antagonistic to that purpose or serves other purposes, it should not be allowed. In that vein, the GC calls to prohibit the profiling or targeting of children for commercial purposes.[92] In our view, the call should be implemented without delay. It is inappropriate for EdTech providers to build profiles of children to predict or influence their attitudes or behaviour for commercial gain, as this is equivalent to exploiting and manipulating children in the very environment that should foster their acquisition of knowledge and the development of their critical thinking skills.

(c) Lack of compliance

Another recurring theme in 5Right's previous literature is the lack of government guidance and oversight for EdTech. As a potential avenue to be explored, it has been suggested that joint inspections could be carried out by Office for Standards in Education, Children's Services and Skills (**Ofsted**) and the ICO, the former focusing on utility and the other on compliance with data protection laws.[93] Another potential avenue involves exploring whether the Office of Qualifications and Examinations Regulation (**Ofqual**) could have an extended mandate to apply its expertise "to assessing the appropriateness of Learning EdTech tools used for assessments and predicting grades".[94]

[92] Ibid.
[93] Ibid 41.
[94] Ibid 44.

(d) Applicability of AADC

There seems to be confusion and conflicting views among experts on the applicability of the AADC to EdTech and schools.[95] Often, the EdTech service is provided through an intermediary, such as a school, but it is not offered directly to the child. It has been suggested that the AADC does not apply where the school acts as an intermediary, such as when EdTech tools are used at school or home at the school's request (for homework, for example).[96] The ICO should provide more detailed guidance on applying the AADC to education data.[97]

As asserted above, in our view, the AADC ought to apply to EdTech and schools. Therefore, it would be useful for the ICO to provide an unequivocal statement clarifying that the AADC applies to EdTech.

(e) Lack of evidence, oversight and government guidance

There is currently no evidence-based assessment of commercial Learning EdTech tools for effectiveness or compliance with data protection laws. Schools lack guidance on how to conduct the procurement process. There should be guidance for assessing specific EdTech products and services for effectiveness and impact and a framework for rating products "based on formal evidence rather than anecdotal evidence".[98]

In this vein, the EdTech Hub, a global research partnership founded in 2019 and run collaboratively by some organisations, aims to tackle the barriers that have thus far prevented EdTech from fulfilling its promise of alleviating the worldwide education crisis, including the lack of robust and accessible evidence on EdTech tools and strategies.[99] Part of the EdTech Hub's mission is to 'synthesize existing evidence, conduct new research, support innovations to scale, and provide advisory support to governments and other country partners'. While the EdTech Hub's research appears to focus on developing countries, some of the evidence gathered or the approaches developed to gather that evidence could be useful to school administrators in developed countries.

[95] Ibid 24.

[96] 'Age Appropriate Design Code Applies to EdTech — Defend Digital Me', *Defend Digital Me* (24 October 2020) <https://defenddigitalme.org/2020/10/24/age-appropriate-design-code-applies-to-edtech/>.

[97] Digital Futures Commission (n 5) 24.

[98] Ibid 33–34 See Recommendation 4.

[99] 'Education and Technology' (n 82); 'EdTech Hub', *EdTech Hub* <https://edtechhub.org/>.

Within the UK, as previous research by 5Rights has noted, the government should "develop rules for the procurement of Learning EdTech by schools" and prepare an approved list of compliant companies. In addition, the ICO should "develop standard contractual clauses for contracts between schools and Learning EdTech companies".[100] In a rush to move learning online during the COVID-19 pandemic, compliance has been neglected to ensure access.[101] This imbalance should be corrected as the urgency brought by the lockdowns subsides and EdTech tools become more firmly incorporated in schools' regular curriculum delivery methods.

The Ethical Framework for AI in Education could inspire development such as an evaluation and procurement process.[102] However, the assessment of Learning EdTech tools should follow a life-cycle approach rather than a one-off approach. EdTech tools used in schools should be re-evaluated whenever developers bring significant modifications to them and, in any event, should undergo periodic evaluation and be compared with new products on the market.

(f) Public interest

It is not clear how data should be shared in the public interest. Some options that may be explored include requiring EdTech companies to "share data with the DfE and ONS [Office of National Statistics], to be included in the NPD [National Pupil Database] and accessed by accredited researchers", or to "share their data with government-managed data trusts for use in the public interest". Another avenue is to explore "open standards for learning environments from other jurisdictions".[103]

[100] Digital Futures Commission (n 5) 37–44 See Recommendations 5, 7, 9.
[101] Ibid 44–45.
[102] Ibid 38.
[103] Ibid 48.

2.8 Recommendations

It has been suggested that compliance with the highest data protection and child rights standards would help the UK secure its place as a leader in the global education marketplace.[104] We should aspire to this leadership role not so much to stimulate the creation of a vibrant EdTech, but rather because children in this country deserve nothing less. We strongly support the previous recommendation that "States need to commit to enabling children to connect at home and school; to support teachers in finding meaningful ways to integrate technology into the classroom; and to invest in the digital literacy of children and their parents and carers."[105] Tackling this issue involves building and investing in "basic infrastructure, including electricity, computers and the internet, as well as remedying teachers and parents" lack of proficiency in digital technologies.[106]

Children themselves recognise the role of technology in their education

In a study surveying children's views from around the world on their digital rights, children showed an acute awareness of the primordial role of technology in their development, growth, education, and eventual career prospects. Indeed, children readily identified the potential of digital technology to strengthen their right to education.[107] Children recognised the advantages of digital technology "for children living in remote areas, or those who are unable to physically attend a school, including children in a humanitarian crisis",[108] as well as its potential for "improving access for children with disabilities, creating opportunities for self-directed learning, and providing effective and engaging learning tools for research and schoolwork."[109]

[104] Ibid 45.
[105] Amanda Third and Lilly Moody, *Our Rights in a Digital World: A Snapshot of Children's Views from around the World* (March 2021) <https://5rightsfoundation.com/uploads/Our%20Rights%20in%20a%20Digital%20World.pdf>.
[106] Ibid 98.
[107] Ibid.
[108] Ibid 95.
[109] Ibid 96.

Children explained that these digital technologies were integral to their formal and informal learning experiences.[110] They "highlighted the importance of digital literacy skills for their capacity to maximise the educational opportunities afforded by digital technologies."[111] Children expressed varied levels of confidence in their digital literacy skills. Low confidence seemed to stem from "limited access to digital technologies at home and at school or from lack of opportunities to acquire digital literacy skills", with many children from both high- and low-income countries noting that their school failed to teach them important skills and that teaching staff often lacked knowledge in these areas.[112] Nevertheless, children realised the vital role of digital technology and digital literacy in achieving their dreams and reaching their full potential in the 21st century's digital economy.[113]

Similarly, children "demonstrat[ed] a sophisticated understanding of the holistic skill sets needed to navigate the digital environment for maximum benefit, [...] identif[ying] digital citizenship skills, such as tolerance, respect, and critical thinking, alongside technical skills, such as typing and coding, as being amongst the most important skills for the digital age."[114]

Strategies for improving education through EdTech

EdTech is not a magic bullet,[115] nor is it, by itself, a panacea.[116] Despite acknowledging this, Alejandro Ganimian, Emiliana Vegas, and Frederick Hess argue that EdTech can complement teaching and learning when used 'smartly'.[117] Their research, focusing mostly on low- and middle-income countries, has led them to conclude that attempts to harness EdTech have not paid sufficient attention to what they identify as technology's four comparative advantages over traditional classroom instruction, namely:

[110] Ibid.
[111] Ibid 97.
[112] Ibid.
[113] Ibid 98.
[114] Ibid 97.
[115] Ganimian, Vegas and Hess (n 79).
[116] 'Education and Technology' (n 82).
[117] Ibid See video linked on page.

'Scaling up quality instruction, such as through pre-recorded quality lessons', 'enabling distance education (e.g., for learners in remote areas and/or during school closures)' and 'distributing hardware preloaded with educational materials'. Studies concerning these strategies showed promising, though inconclusive, results. Gaminian et al caution that '**part of the reason why they have proven effective is that the "counterfactual" conditions** for learning (i.e., what would have happened to learners in the absence of such programs) **was either not to have access to schooling or to be exposed to low-quality instruction.**' Thus, it may be inappropriate to take similar interventions where learners do not find themselves in similar situations. In our view, this is an important point for UK schools to keep in mind when considering whether to incorporate 'scaled up' quality instruction in the EdTech strategies. Where the alternative is not the absence of schooling or low-quality schooling, the switch to pre-recorded or distance instruction may have more drawbacks than selling points. It may have an overall negative impact on the learning experience.

'Facilitating differentiated instruction, through, for example, computer-adaptive learning and live one-on-one tutoring.'

Computer-adaptive learning refers to 'instruction and opportunities for practice that adjusts to each individual's level and pace of preparation.' Ideally, the system 'diagnose[s] students' initial learning levels and assign[s] students to instruction and exercises of appropriate difficulty' and then continues to adjust the level of difficulty after each question depending on whether the student answered correctly (this is referred to as 'dynamic adaptation'). This individualisation truly harnesses the power of technology. It is something no single educator, 'no matter how talented', would be able to provide simultaneously to each student under their care.

'Expanding opportunities to practice.'

The authors explain that 'Technology can help learners get more out of traditional instruction by providing them with opportunities to implement what they learn in class.'[118]

'Increasing learner engagement through videos and games.'

[118] Again, however, they note that existing evidence of this strategy as deployed in developing countries show mixed results, reflecting both promise and limitations. It is difficult to isolate the effect of interventions as they often incorporate confounding factors, such as allowing for peer-to-peer collaboration and additional instruction time (as the interventions expanding practice opportunities often took place before or after school, thus increasing the total time spent learning).

Ganimian et al suggest that video tutorials for self-paced learning and gamified practice/exercises could potentially address the challenges raised by large class sizes. Ganimian et al propose a three-step approach to education technology. The first step is the **diagnosis**: it involves 'understanding [ing] the needs, infrastructure, and capacity of a school system'. The second revolves around the **evidence**: it requires considering 'the best available evidence on interventions that match' the conditions of that school system. The third step, the **prognosis**, requires 'closely monitor[ing] the results of innovations before they are scaled up', allowing for adjustments to be made in real-time.

The authors have also put forward 'five specific and sequential guidelines for decision-makers to realize the potential of education technology to accelerate student learning', which, while they were developed with developing countries in mind, may offer useful reflection points to school administrators in developed countries such as the United Kingdom. These guidelines encourage administrators to (1) assess how their schools, educators, and learners are currently engaging with technology by carrying out a short in-school survey to identify regulations, policies, or physical barriers that might limit technology use in a particular school environment. (2) Administrators should '[c]onsider how the introduction of technology may affect the interactions among learners, educators, and content', as interventions that do not impact these interactions are unlikely to improve learning and may represent a poor investment of resources, especially considering that they can be quite costly. (3) They should then delineate clear objectives and determine how progress towards these goals will be measured and adjusted. (4) Next, the authors emphasise the importance of considering the input of educators and families and paying attention to how technology will be used because new or ineffectually used technology inevitably leads to disappointing results, regardless of how virtuous the technology is in question may be. In other words, '[*h*]*ow* this kind of reform is approached can matter immensely for its success.' Finally, the authors insist that '[i]t is essential to communicate with stakeholders, including educators, school leaders, parents, and learners.'[119]

[119] Under this rubric, the authors make a key point about making allies, not alienating stakeholders: 'Technology can feel alien in schools, confuse parents and (especially) older educators, or become an alluring distraction. Good communication can help address all of these risks. Taking care to listen to educators and families can help ensure that programs are informed by their needs and concerns. […] For instance, if teachers fear that technology is intended to reduce the need for educators, they will tend to be hostile; if they believe that it is intended to assist them in their work, they will be more receptive.'

Beyond academia, contributions to developing strategies for promoting the right to education through EdTech have also come from financial institutions. The World Bank Group is 'the largest financier of education in the developing world', operating 'in partnership with governments and organizations worldwide to support innovative projects', including EdTech. The World Bank expressed concern that the COVID crisis could exacerbate already high levels of 'learning poverty', which it estimates 'by measuring the number of 10-year-old children who cannot read and understand a simple story by the end of primary school'. The World Bank proposes three areas of focus for tackling the inequalities in digital access highlighted by the pandemic:

- digital infrastructure (connectivity, devices and software);
- human infrastructure (teacher capacity, student skills and parental support); and
- logistical and administrative systems to deploy and maintain tech architecture.

The World Bank acknowledges that teachers are as crucial, if not more, to learning in tech-rich environments. That evidence has shown that bypassing them when implementing education technology bars improvement in student learning. The approach supported by the World Bank involves 'support[ing] the design and development of new educational content and curriculum' and of 'new open educational libraries', as well as the definition of '21st-century competencies in students and teachers' and the identification of 'ways to more effectively measure these skills and accredit [them]'.

It is also worth highlighting the five principles that make up the World Bank's EdTech Strategy.[120] Some of them echo the themes present in recommendations put by Ganimian et al. The five principles are the following: (1) **'ask why'** (developing EdTech policies with a clear purpose, strategy, and vision, and framing EdTech as a means to an end – that of supporting the 'human-centred socially intensive endeavour' that is education) rather than end onto itself); (2) **'design for scale'**, with an eye on flexibility, equity and inclusion to avoid EdTech's usual tendency of exacerbating inequities in education systems; (3) **'empower teachers'** (i.e. using technology to 'augment teaching' rather than replace teachers, 'enhanc[ing] teacher engagement with students', helping to fill gaps in teachers' knowledge and to build their skills where necessary, but mostly allowing them to focus on more sophisticated tasks that draw on their expertise and humanity)[121]; (4) **'engage the ecosystem'**, defined broadly as encompassing 'key stakeholders such as students, teachers, school leaders, parents, NGOs, donors and the private sector including app developers, publishers, equipment manufacturers, telecommunication companies and cloud service providers', thus prompting education systems to adopt and whole-of-government and multi-stakeholder approach'; and (5) **'data driven'**, referring to development of '[t]ransparent standards and interoperable data architecture [which] support[] evidence-based decision making and a culture of learning and experimentation'. On this last point, while we agree that evidence-based decision-making should be promoted and interoperability and transparency are laudable goals, we note that this view lacks awareness of and sensitivity to data protection. As we discuss elsewhere in this report, ensuring robust protection for student's privacy and data in the deployment of EdTech is key to ensuring respect for children's digital rights.

The principled strategies put forward by the researchers at the Brookings Institute and the World Bank described above illustrate how different thinkers and actors propose that EdTech be implemented. The successful implementation that these approaches seek to achieve is key to ensuring that EdTech will, in fact, promote children's right to education.

[120] 'Education and Technology' (n 82).

[121] We note that this mirrors Ganimian's emphasis on the 'instructional core', of which educators form a key component.

3 Violence against children and criminal exploitation

In their interaction with the digital environment, children are exposed to myriad forms of violence and exploitation. Unless protective in nature, technological restrictions will hinder digital participation, which is important for accessing information and entertainment. However, unchecked, increased exposure to this digital environment carries its attendant risks to children's physical and mental health. In the context of the current legal framework, there is a need to introduce regulation of the content deemed to be acceptable. Minimum age limits, pre-moderated content for minors, default protections for under-age accounts, swift management of inappropriate/illegal content, efficient identity and age-verification authentication solutions can assist with this regulation. Alongside a robust parental control system, children themselves should also be able to report inappropriate content easily. This can be made possible through accessible laws and policies and a strong local support network. Privacy controls should operate so that only the data relevant to the purpose is collected. In addition, information about the type of information collected and the duration of storage should be provided to the data subject. Given default privacy, a reasonable choice about how specific data (e.g., geolocation data) will be used should be provided. There is a need for greater parental involvement for children under 18 years of age, with strict privacy measures for those under 13. A strong culture of education about the advantages of digital platforms as well as an awareness of the harms of unregulated online exposure is the correct path forward.

3.1 Background

Children's interaction with the digital environment currently exposes them to unique risks of online harm. Criminal targeting and harm caused to children in the digital environment take place mainly in the form of abuse and exploitation. Examples include online sexual exploitation and abuse, modern slavering and human trafficking, and online extremism or radicalisation.[122]

[122] Department for Education, *Working Together to Safeguard Children* (2018) <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>; Department of Health Northern Ireland, *Co-Operating to Safeguard Children and Young People in Northern Ireland* (25 March 2016) <https://www.health-ni.gov.uk/publications/co-operating-safeguard-children-and-young-people-northern-ireland>; Minister for Children and Young People, *National Guidance for Child Protection in Scotland 2021* (2021) <http://www.gov.scot/publications/national-guidance-child-protection-scotland-2021/>; Home Office, *Tackling Violence against Women and Girls Strategy* (2021) <https://www.gov.uk/government/publications/tackling-violence-against-women-and-girls-strategy>; Cardiff and the Vale of Glamorgan Regional Safeguarding Board, 'Wales Safeguarding Procedures', *Welsh Government* (2020) <https://www.safeguarding.wales/>.

A distinction can be drawn between contact abuse and non-contact abuse. The former involves physical contact and entails, inter alia, sexual touching of body parts (with/without clothes), online sexual harassment (through comments/jokes/content-sharing),[123] extreme pornography, deep-fake pornography (deliberately sending false and threatening content), cyber-flashing (sending unsolicited images of genitalia), coercion or encouragement to partake in sexual activities, or any form of rape or penetration that results in violence towards children. Non-contact abuse includes but is not limited to exposing children to sexual activities, circulating, viewing or making images or videos, and any form of exploitation for power, status or money.[124]

3.2 Digital participation and potential harm – an overview

Increasing recognition of digital participation rights has sparked a shift away from a regime of unjustifiable policing. Unless protection is justifiably enhanced through restrictions, the critical role of digital media in communication, receipt of information and self-expression must be recognised. Undoubtedly, digital participation enables children to access information and knowledge sources.[125] In addition, it is crucial to access online mental health support, therapy and/or counselling, particularly amidst a global pandemic.[126]

[123] Department for Education, *Keeping Children Safe in Education* (September 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014058/KCSIE_2021_Part_One_September.pdf>.
[124] Department for Education, 'Working Together to Safeguard Children' (n 122); Department of Health Northern Ireland (n 122); Minister for Children and Young People (n 122); Home Office, 'Tackling Violence against Women and Girls Strategy' (n 122); Cardiff and the Vale of Glamorgan Regional Safeguarding Board (n 122).
[125] Eva Lievens et al, 'Children's Rights and Digital Technologies' in Ursula Kilkelly and Ton Liefaard (eds), *International Human Rights of Children* (Springer, 2019) 487 <https://doi.org/10.1007/978-981-10-4184-6_16>.
[126] Daniel Kardefelt-Winther, 'Responding to Screen Time Concerns: A Children's Rights Approach - Evidence for Action', *UNICEF* (17 April 2019) <https://blogs.unicef.org/evidence-for-action/screen-time-concerns-children-participation-digital-online/>.

Notwithstanding the positive effects, increased use of the internet results in a wider engagement with online activities that carry their own risks. There can be exposed to harmful content when seeking information online. This includes gender-based violence and sexual objectification. Resulting negative outcomes include depression, anxiety, panic attacks and suicidal thoughts/behaviours.[127] Thus, digital participation should be encouraged but with more awareness of the potential risks and harms of unregulated internet access.

3.3 Child rights opportunities and impacts

(a) Non-discrimination

The internet has become a powerful way of overcoming discrimination and other forms of exclusion by providing children with a tool for meaningfully participating in decision-making processes and exercising their rights.[128]

However, despite the opportunities that digital access opens up, the universal language of the UNCRC fails to account for the differences between the Global North and the Global South. This is noticeable when examining differences in, for instance, internet access and the extent of parental supervision. While the right to participation and play is enshrined in the UNCRC, the instrument's universal language at times fails to correspond to the diversity of factors that shape communications technologies and how children experience the digital environment. For instance, the differences in access to the internet and the extent of parental supervision vary greatly worldwide. Thus, to be valuable, strategies need to consider the contexts in which they operate.[129]

[127] Mariya Stoilova, Sonia Livingstone and Rana Khazbak, *Investigating Risks and Opportunities for Children in a Digital World: A Rapid Review of the Evidence on Children's Internet Use and Outcomes* (Innocenti Discussion Paper, February 2021) <https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf>.
[128] Kardefelt-Winther (n 126).
[129] Alexandra Chernyavskaya, 'Children's Rights in the Digital Age', *London School of Economics and Political Science* (2015) <https://www.lse.ac.uk/media-and-communications/events/past-events/childrens-rights-in-the-digital-age.aspx>.

(b) Best interests of the child

There is a need for an integrated, rights-based perspective concerning children's engagement with digital technologies. Protection of the child's best interests under Article 3 of the UNCRC requires drawing on their experiences and circumstances.[130] No hierarchy of rights should exist, and protection rights should be equal to participation and play rights. As noted in Article 12 of the UNCRC, children should be consulted, depending on their age and maturity, on issues concerning their use of digital technologies. Schools should teach children to question, not to accept what the authority tells them is right automatically. They should be trained to search for accurate, high-quality information and be able to distinguish credible information from fake content. Increasing the exercise of their own views and judgement will help psychologically healthy and socially responsible citizens.[131]

(c) Right to life, survival, and development

The CRC recognises children's inherent right to life and imposes an obligation on States to ensure the child's survival and development to the maximum extent possible.[132] Relatedly, the CRC obliges States to take appropriate measures to protect children from all forms of violence or exploitation prejudicial to any aspects of the child's welfare.[133]

The digital environment creates new ways of perpetrating or promoting such violence against children. This is of grave concern, especially given the increased time children spend online due to the COVID-19 pandemic.

Box 9: Risks of online exploitation

Digital technologies like video streaming can be used to produce and distribute sexually abusive or exploitative information. This can, in turn, lead to sexual extortion, cyberbullying, threats to reputation, creation and sharing of non-consensual texts and images, and soliciting or coercing children to generate such content themselves. Serious consequences include "physical or mental violence, injury or abuse, neglect or maltreatment, exploitation, and abuse, including sexual exploitation and abuse, child trafficking, gender-based violence, cyberaggression, cyberattacks and information warfare".[134]

[130] {Citation}
[131] Kardefelt-Winther (n 126).
[132] *CRC* (n 1) art 6.
[133] Ibid art 19, 36.
[134] *General Comment No. 25* (n 2) [82].

This harm is further compounded when considering that the child victims of such crimes also encompass vulnerable children, such as migrant or refugee children or children with disabilities (including those who have epilepsy and are subjected to online flashing images, covered by Zach's law).[135] A delicate balance must be struck between preventing children's exposure to all forms of online exploitation and ensuring that their protection does not ultimately lead to their exclusion. This consideration is particularly pertinent with respect to children from vulnerable and already marginalised backgrounds.

(d) Respect for the views of the child

As noted in Article 12 of the UNCRC, children should be consulted, depending on their age and maturity, on issues concerning their use of digital technologies. Schools should teach children to question rather than accept what the authority tells them is right automatically. They should be trained to search for accurate, high-quality information and be able to distinguish credible information from fake content. Increasing the exercise of their views and judgement will help develop psychologically healthy and socially responsible citizens.

(e) Civil rights and freedoms

Freedom of expression and access to information

One key set of rights that should be carefully considered when applying digital technology to protect children from criminal exploitation are those pertaining to freedom of expression and access to information under Articles 13 and 17 of the CRC, respectively. As highlighted by the GC, the digital environment can include "gender-stereotyped, discriminatory, racist, violent, pornographic, and exploitative information, false narratives, misinformation and disinformation and information encouraging children to engage in unlawful or harmful activities".[136] In protecting children from this harmful material, states should ensure that relevant businesses and other digital content providers develop and implement guidelines to enable children to access safely diverse content in recognising children's right to information and freedom of expression, rather than excluding them from digital spaces altogether.

---

[135] The eponymous law was enacted after an eight-year-old boy, Zach Eagling, was trolled for suffering from epilepsy and cerebral palsy. The offence covers flashing images on social media platforms that are intended to cause seizures. As recently as July 2021, the UK Law Commission recommended the introduction of a special offence to deal with flashing images that intend to cause seizures to people suffering from epilepsy. Epilepsy Society, *Tackling Online Abuse: Written Evidence Submitted by the Epilepsy Society (TOA0020) Zach's Law: Protecting People with Epilepsy from Online Harms* (August 2021) <https://committees.parliament.uk/writtenevidence/10069/pdf/>.

[136] *General Comment No. 25* (n 2) [54].

Moreover, technologies should facilitate the sharing of experiences by these victims or survivors. Finally, any restrictions should be lawfully necessary and proportionate, whether through filters or safety measures.

Box 10: Potential balancing of rights in a digital environment

An instance of technologies operating necessarily and proportionately would be when children's creation and sharing of digital content is encouraged, but not at the cost of violating other people's dignity or inciting hatred or any form of violence. Otherwise, when children create and share non-infringing content expressing their experiences and views, the State is obliged to protect them from "criticism, hostility, threats or punishment".[137] Other threats include "cyber aggression and threats, censorship, data breaches and digital surveillance".[138]

3.4 General measures of implementation by the United Kingdom

(a) Legislation

A range of legislation addresses the various aspects of criminal exploitation of children in the digital environment. For example, the Children Act 1989 and the Children Act 2004 broadly cover child needs and services to ensure general welfare.[139] However, their online protection is largely covered by laws and policies derived from the Data Protection Act, 2018 (DPA). Superseding the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 provide an updated legal framework to ensure the smooth and safe sharing of personal information. The laws do not limit the sharing of information but ensure that all processing conditions are followed and that due consent is obtained (legally sharing information without consent if obtaining the same is not possible).[140]

[137] Ibid [60].
[138] Ibid.
[139] David Foster, *An Overview of Child Protection Legislation in England* (4 July 2018) <https://commonslibrary.parliament.uk/research-briefings/sn06787/>.
[140] UK Government, 'Information Sharing Advice for Safeguarding Practitioners', *House of Commons Library* (19 February 2020) <https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>.

Digital Economy Act 2017

The Digital Economy Act 2017 (**DEA**) was enacted to regulate access to pornography in the digital environment. It ensures that commercial websites employ sophisticated age-verification measures to deny access to those under 18 years of age mandatorily. An age verification regulator has been entrusted with the statutory task of oversight to ensure proper compliance. Moreover, the regulator can impose enforcement measures, including punitive sanctions, on the non-compliant party. However, major gaps appear upon analysing its provisions in relation to its scope and effectiveness.[141]

Age Appropriate Design Code 2020

The AADC, also known as the Children's Code, was released by the Information Commissioner (ICO). Taking effect on 2 September 2021, it served as a 12-month transition and acted as a guide to protect children's personal data on online platforms.[142] A statutory practice code prepared under Article 123 of the DPA contains 15 standards in place to protect the best interests of the child.[143] It recommends that the providers of 'information society services' adhere to these standards if their services are accessed by those under 18 years of age in the UK. This includes appropriate age-verification systems that are proportionate to the potential risk of harm that they are exposed to. If the personal data of children in the UK is being processed, it is irrelevant whether the company is based in the UK or not.[144]

The Code suggests that there be no profiling by default, and the same should be activated by explicit user consent. The default option should be allowed only if a compelling reason for profiling is shown. Moreover, such profiling should come with adequate safeguards against the potentially harmful effects of the content.[145]

Box 11: Gangs Matrix and data privacy laws

[141] Majid Yar, 'Protecting Children from Internet Pornography? A Critical Assessment of Statutory Age Verification and Its Enforcement in the UK' (2019) 43(1) *Policing: An International Journal* 183 <https://doi.org/10.1108/PIJPSM-07-2019-0108> ('Protecting Children from Internet Pornography?').

[142] Jane Bird, 'The ICO's Children Code: Do You Need to Comply?', *Protecture* (4 May 2021) <https://protecture.co.uk/icos-childrens-code/>.

[143] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58).

[144] Ibid.

[145] Simone van der Hof et al, 'The Child's Right to Protection against Economic Exploitation in the Digital World' (2020) 28(4) *The International Journal of Children's Rights* 833.

In 2018, Amnesty International released a report highlighting the risks posed by labelling mostly BAME groups as 'gangs' in the UK.[146] The Metropolitan Police Service Gangs Violence Matrix, an institutional database, has been created to compile a list of suspected gang members linked to violence. The racialised nature of the database has also been highlighted, with mostly BAME groups being labelled as 'gangs' in the Matrix.[147] This results in the overidentification and digital profiling of mostly young BAME adults, which has, in turn, led to their stigmatisation and undue policing as 'high-risk' individuals. Worryingly, Section 29 of the DPA allows exemptions from data protection principles for crime prevention.

Moreover, Section 26 of the RIPA requires a sanction for any form of direct intrusion into personal information. Thus, privacy controls should not be easily bypassed for social media monitoring. This data matrix must be done away with unless it complies with domestic and international instruments on data protection. Robust data sharing agreements with government agencies and local authorities should be in place for clear data retention and processing guidance. This approach can also reform children's data usage in algorithm policing.[148]

Online Safety Bill 2021

In 2021, the UK Government introduced the Draft Online Safety Bill ('the Bill') to protect children online.[149] The Bill represents the UK Government's response to the Online Harms White Paper and associated consultations.[150] It places a greater responsibility on social media intermediaries (including websites, applications and other such hosts providing services) to curb the circulation of sexually exploitative content, racially abusive matters, suicide-related information, and terrorist material.

[146] Amnesty International, *Trapped in the Matrix* (2018) <https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf>.
[147] Ibid.
[148] Ibid.
[149] *Draft Online Safety Bill 2021* (CP 405).
[150] Home Office, *Online Harms White Paper: Full Government Response to the Consultation* (December 2020) <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper>.

The Bill appoints Ofcom, an independent regulator, to hold platforms accountable to this new statutory duty of care. Any company allowing for the discovery or sharing of user-generated content or any other online interaction is captured within the ambit of Bill's obligations. These include search engines, public discussion spaces, file hosting websites, media platforms and messaging forums. Enforcement tools based on this mandatory duty of care allow for substantial fines, impose liability on individuals in the senior management of companies, and even block access to those websites. Other notable measures apart from this statutory duty of care include a requirement for social media sites to publish annual transparency reports on the steps being taken to address large volumes of harmful online content, expeditious redressal of user complaints, use of safety by design features, and a media literacy campaign to raise awareness about online threats.[151]

Interim Codes on Child Sexual Abuse Material and Terrorist Content

In 2020, the UK Government released an interim code offering specific practical solutions to online child sexual exploitation and abuse.[152] A similar interim code was released for terrorism-related content[153] defined in the Terrorist Acts 2000 and 2006.[154] With identical strategies and suggestions, it focuses on expeditious identification and removal of terrorist content, using a mixture of automated technologies and human supervision. With a high level of user compliance for removal and retention requests by authorities, holistic cooperation systems are recommended.

[151] Department of Digital, Culture, Media & Sport, 'UK to Introduce World First Online Safety Laws', *UK Government* (8 April 2019) <https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws>.

[152] Home Office, 'Interim Code of Practice on Online Child Sexual Exploitation and Abuse (Accessible Version)', *UK Government* (15 December 2020) <https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual-exploitation-and-abuse-accessible-version>.

[153] This has been interpreted to include direct or indirect encouragement or other inducement, including the glorification of commission, preparation, or instigation. It involves belonging to a proscribed organization and expressing their opinions and beliefs, or publishing any image, clothing item or article of that organization. Collection, recording, providing/receiving invites or training for making/using weapons and/or explosives is also covered. Lastly, sharing of propaganda through media channels, live broadcasting, posting URL's or third-party content/activity, and making and/or selling terrorist publications also invites the existing laws.

[154] Home Office, 'Interim Code of Practice on Terrorist Content and Activity Online (Accessible Version)', *UK Government* (15 December 2020) <https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-terrorist-content-and-activity-online-accessible-version>.

(b) Comprehensive policy and strategy

The Committee on the Rights of the Child reviews comments made by NGOs and other institutions during its ongoing reporting cycle. This includes supporting the government in its response to the recommendations of the Committee.[155] Since the inclusion of children in laws and policies is crucial, the following suggestions on privacy protection and management settings were raised in an earlier report published by the 5Rights Foundation.[156]

- Enacting robust laws and regulations that give children a choice in data collection, storage, and distribution by companies. The legal framework should prevent companies from releasing private information without children's permission.

- Incorporating greater transparency in the processes of data collection and usage by companies through, for example, the presence of simplified legal texts and user agreements would make it understandable for children.

- Ensuring greater control of the given data, including the right to be forgotten. During data collection, companies collecting information should specify who the information would be shared with and for which purposes.

- Regularly notifying users of the collection, storage, and usage. A monthly notification of how the collected and saved data has been used should be provided. Tools like caches and cookies should be employed to make it easier for users to opt-out of agreeing to their usage. The access to information on those platforms should then not be restricted for failure to accept the concerned cookie policy.

- Overhauling the approach favouring a default privacy protection approach - rather than the settings agreeing to personal data collection, the default should be set to a 'No', allowing for data collection only with user consent.

- Providing greater education on privacy settings to secure personal data.

On the aspect of violence, the following recommendations were made.

[155] 'Child Rights Connect: CRC Reporting Cycle | Working with the UN CRC Reporting Cycle' <https://crcreporting.childrightsconnect.org/> ('Child Rights Connect').
[156] 5Rights Foundation, *Pathways: How Digital Design Puts Children at Risk* (5Rights Foundation, July 2021) 108.

- Spelling out the various kinds of safety concerns related to inappropriate content. These should include cyber-bullying, harassment (including sexting and circulation of naked pictures that had initially been sent privately), discrimination, exposure to violent or sexual content, sexual exploitation, online trafficking, mental health impacts, catfishing, child pornography, online extremism/radicalisation, and even kidnapping and murder, the commission of all of which begins on the internet. Race and gender-related assaults, including aggressive homophobic comments, death threats and exposing someone to ridicule and embarrassment, must also be included. This open-ended list must be continually updated to keep abreast of new risks and harms in this information age.

- Expanding the scope of inappropriate content to include news coverage that is disturbing and violent live-streamed content.

Another novel policy solution to the problem mentioned above of exploitation is to conduct regular rights-impact assessments. This will help protect the best interests of the child and help involve children when considering the range of rights to be protected. When looking at children of different age groups with different maturity levels, their evolving capacities can then be considered. In addition, privacy-by-design is crucial for default data minimisation. This default non-collection ensures that children and parents do not have to be acquainted with complex data processing technologies.

Moreover, transparency central to data processing services will ensure that users are notified of any significant changes in processing systems. Furthermore, profiling systems can be operated to automatically exclude the personal data of those under 18 years of age. This approach could, in turn, be applied even to commercial activities and business responsibilities.[157]

To regulate access to sexually explicit content, age-verification systems need to have strict checks on identification documents to catch fake passwords that are illegally acquired and used to bypass mandatory age-verification mechanisms. Sophisticated technologies need to be employed to catch the usage of VPNs to bypass age-verification systems. Verification providers, including third-party providers, need to have robust privacy settings that protect personal information. Finally, a separation between verification providers and the internet platforms needs to be maintained to prevent abuse of user data.[158]

[157] van der Hof et al (n 145).
[158] Yar (n 141).

Companies must take appropriate action to report content that seeks to exploit children criminally. Some policy steps that can be adopted include strict terms of service, prompt identification of inappropriate content, preventing abusive search content from appearing, strong action against live streaming of sexually illicit content and operational reporting to the appropriate authorities. Reporting options must include context that seems harmless but is harmful when seen in the relevant context. The design and development of technological systems and processes must consider this evolving landscape. Collaboration among companies to share data, tools and techniques is pivotal to combat criminal exploitation by responding to threats more effectively.[159]

3.5 Gaps in current frameworks

The present legal regime insufficiently protects children's digital rights. The online legal setup must cater to their special needs and interests. Given how the freedom of expression is amplified with the rise of online legal platforms, individuals and organisations are not being held to account for their actions. Law enforcement cannot keep up with the rapid pace of online harm (ex: child grooming, racial hate, cyberbullying, dissemination of extreme pornography etc.). The responsibility of parents and the general duty of care for third party internet users is not strong enough to protect children's privacy on the internet. Indeed, the threat is not just to children but to the idea of childhood as well. Digital services' technological design and architecture operate with commercial interests in mind, thereby disregarding their data protection obligations. Ultimately, a balance must be drawn between protecting children from online risks and harms and enabling them to exercise their digital rights.[160]

A crucial goal is to ensure access to justice and remedies. Certain key impediments exist:

- Lack of sanctions in legislation for child rights abuses.
- Problems with obtaining evidence or determining the perpetrators due to inadequate knowledge about the threshold of what constitutes an 'abuse' or 'violation'.
- Difficulties in the 'complaint and reporting mechanism'.

[159] Bruce Zagaris, 'Online Child Sex Exploitation Abuse' (2020) 36(4) *International Enforcement Law Reporter* 161 <https://heinonline.org/HOL/Page?handle=hein.journals/ielr36&id=169&div=&collection=>.
[160] Sonia Livingstone, 'Implementing Children's Rights in a Digital World', *Parenting for a Digital Future* (27 November 2019) <https://blogs.lse.ac.uk/parenting4digitalfuture/2019/11/27/implementing-childrens-rights-in-a-digital-world/>.

- Nature of claims should include class action and other such public interest litigation
- Inadequate rehabilitative care, including frameworks for therapy, follow-up care and social re-integration.
- Nature of reparations should include "restitution, compensation and satisfaction and may require an apology, correction, removal of unlawful content, access to psychological recovery services or other measures".[161]
- Law enforcement should seek to improve digital technologies to improve the process of investigation and prosecution, among other stages.
- Business enterprises should have robust complaint mechanisms without precluding access to the remedies provided by the state.
- Children should be provided with information through a language and appropriate manner and take individual sensitivities into account.

(a) Scope

There are numerous concerning gaps in the scope of the legislative framework in relation to protecting children from the online harm of sexual exploitation and abuse. Turning first to the DEA, this legislation only covers websites which predominantly display pornographic content.[162] Consequently, websites showing a mixture of pornographic and non-pornographic content remain unencumbered by the obligation under the DEA to employ sophisticated age-verification measures to deny access to those under 18 years of age. This effectively allows websites to circumvent the law by simply displaying sexual content that may not fall within 'pornography' as defined by the DEA, thereby allowing free accessibility to children to the harmful, pornographic content alongside the non-pornographic content. What compounds this problem is that content generated by the user does not fall within the ambit of pornographic content.[163] As long as the platform itself does not share the content, it is not unlawful. While many social media platforms have prohibited the sharing of sexually explicit content, dissemination of pornographic content is possible through the bypassing of age verification systems. This is detrimental as pornographic content can be freely circulated among users and escape liability due to the platform not featuring it.

[161] *General Comment No. 5 General Measures of Implementation of the Convention on the Rights of the Child 2003* [24].
[162] Yar (n 141).
[163] Ibid.

Even commercial providers of pornographic content that the DEA catches verification systems can be easily bypassed. Minors often use others' ages to confirm identifications (e.g., credit cards). Moreover, such access is restricted to minors only in the UK, thereby allowing from internet protocol addresses from outside. Thus, virtual private networks (VPNs) may easily be used to also choose addresses from countries of their choice, thus undercutting any protections put in place by the DEA.

A noticeable loophole in scope also exists in the AADC in the form of the exceptions to platforms that constitute 'information society services' (ISS). An ISS has been defined as:

> "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[164]

Accordingly, online services covered by the AADC are those like "apps, programs and many websites including search engines, social media platforms, online messaging or internet-based voice telephony services, online marketplaces, content streaming services (e.g. video, music or gaming services), online games, news or educational websites, and any websites offering other goods or services to users over the digital environment."[165] However, the following have not been categorised as 'relevant ISS':

- Services offered by public authorities (operated on a non-commercial basis)
- Websites providing information about real-world business or service
- Voice Telephony services
- General broadcast services
- Preventive and counselling service

Consequently, these online platforms are not required to adhere to the standards put in place by the AADC to protect the best interests of the child. The parameters of protection for children in the digital environment should not be unnecessarily limited merely by the commercial nature of operations of online services. Indeed, despite not functioning on a commercial basis or for remuneration, the personnel operating these services can still misuse the same to exploit children criminally. Although, understandably, the same standard cannot be applied, safeguards are still needed to achieve a minimum level of protection for children when they seek these services.

[164] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 14–15.
[165] Information Commissioner's Office, 'Services Covered by This Code', *Age Appropriate Design Code* (14 October 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/>.

(b) Enforcement mechanisms

Another issue is the lack of effective or appropriate enforcement mechanisms to ensure compliance. The enforcement value of the AADC has been criticised as particularly weak, given that it can only issue dire warnings followed by regulatory audits and financial sanctions (up to GBP 17.5 million when the UK GDPR is enacted, or 4% of the turnover, whichever is higher).[166] Furthermore, the AADC merely recommends standards of practice rather than imposing any mandatory obligations.

A different aspect to the problem of ineffective or inappropriate enforcement mechanisms arises from the effect of 'gang' associations on data privacy laws in the UK, including the DPA and the RIPA.

Box 12: Gangs Violence Matrix and discrimination

The Metropolitan Police Service Gangs Violence Matrix database has been heavily criticised for its discrimination against black boys and men. In addition, since the sensitive personal data from those databases are shared with other public agencies, there is a potential breach of private and family life. This system operates by assigning a risk/harm score to suspected gang members, who are then colour coded into red, amber or green (most to least likely to commit an offence). Those in the red label pose the highest risk and are excluded from the benefits of housing, education etc. Vague criteria include considering past arrests/convictions, being victims of violence and suspected interacting with 'gang' members.

These arbitrary parameters have resulted in over-policing. Such heavy stereotypes based on racist assumptions form a part of the problem since most of those who are profiled belong to minority ethnic groups.[167] Apart from questions about the reliability and accuracy of data collection, it is also likely that this data is kept longer than needed for the intended purpose. Furthermore, sharing with partner enforcement agencies exacerbates the potential harm to children, given the absence of safeguards from profiling. There is also a lack of scrutiny on how this data is used since there is no legal requirement under the DPA to conduct a privacy data assessment.[168]

[166] Julian Hayes, 'Online Safety - the ICO's Children's Code', *Open Access Government* (8 September 2021) <https://www.openaccessgovernment.org/online-safety-the-icos-childrens-code/119342/>.
[167] Amnesty International (n 146); Sebastian Klovig-Skelton, 'Met Police Faces Legal Action over Gangs Matrix', *ComputerWeekly.com* (online, 1 February 2022) <https://www.computerweekly.com/news/252512752/Met-police-faces-legal-action-over-Gangs-Matrix>; Damien Gayle, 'Rise in Proportion of BAME Suspects on Met's Gangs Matrix', *The Guardian* (online, 29 May 2018) <https://www.theguardian.com/uk-news/2018/may/29/rise-in-proportion-bame-suspects-met-police-gangs-matrix>.
[168] Amnesty International (n 146); Klovig-Skelton (n 167); Gayle (n 167).

(c) Economic exploitation

The regulation of economic exploitation of digital child labour remains sorely neglected and unaddressed, despite its significant overlap with aspects of sexual exploitation. For instance, recruiting child social media influencers to sell goods and services has become popular. At the same time, parents may play a part in these activities, such as assisting with their dressing up and video-editing. In most cases, there is a lack of parental oversight. Even e-Sports has become a way of earning money. However, it is fraught with risk. The activities that children engage in may not always constitute 'play' within the meaning of the CRC. In fact, the exploitative contracts may become a new form of child labour.[169] While it may start out as economic exploitation, the nature of acts (pictures, videos etc.) that children may be coerced into doing in the name of branding might be sexually exploitative. This is expressly prohibited under Article 32 of the CRC. Such emotionally demanding activities need to be regulated to prevent children from suffering from the harmful effects of social media-based employment.[170] The UK's laws and policies need to enact provisions recognising the sexual and criminal aspects of commercial exploitation.

3.6 Recommendations

The legal discourse must shift towards being more participation-oriented to include the right to access information and the freedom of expression. The evolving capacities of children should be given greater attention by linking the online and offline spheres of their lives. Children should receive adequate protection through appropriate mechanisms to report incidents, even if anonymously. In addition, there is a need to disseminate age-appropriate and format-appropriate information, resources and opportunities. Special categories of children (including minorities and differently-abled) should be provided with the same level of protection.[171]

Good practices include using simple language in message/content delivery to the target group. A closed set/walled garden environment for young children is recommended where communications are moderated. In fact, a mix of moderation styles can be employed, including (i) pre-moderation before the content is posted, (ii) post-moderation when the content is posted to see if it is suitable, and (iii) reactive moderation for a prompt investigation into user reports. Parents must be directly involved alongside age-verification systems to ensure constant supervision. Human moderation can help make up for the shortcomings of content filters.

[169] van der Hof et al (n 145).
[170] Ibid.
[171] Lievens et al (n 125).

Along with parental controls, there must be clear warnings before displaying inappropriate content. Online community hosts can help spot subtle risks that can escalate to serious harm (ex: using synonyms of unsuitable language for bullying, soliciting etc.). There should be regular training to raise awareness about online safety in schools. Privacy controls must be age-determined, with enhanced protection for particularly young children (under 13 years of age). A regime of parental control to regulate children's accounts is necessary. All online platforms should impart education and awareness for child protection.[172]

(a) Expanding the scope and clearer definitions

Current legislation and policies do not factor in the need for robust online safety regulations, particularly after the COVID-19 pandemic.

To begin with, the scope of 'child' must be expanded beyond young children in school to encompass young adults who are in and out of care systems. Alongside the Department of Education, other ministries like the Department of Culture, Media and Sport should also shoulder responsibility for wider child rights policies. A participatory child rights approach can implement the right to be heard, information and play in the online space. A shared definition of digital inclusion must be expanded to include a device, a strong connection, skills and support, a safe online environment and sustainable access. This must also include all concerned stakeholders, including schools, parents, support organisations, technology companies, and children. During the pandemic, education, health and social security are predominantly accessed online.

These spheres require greater focus to ensure that all children can realise their rights. For instance, education technology is presently excluded and must be brought within the fold of the UK Online Safety Bill. The scope, including expansive definitions, must be a minimum standard that is reviewed every few years to reflect the changing technological landscape.[173]

[172] UK Council for Child Internet Safety, *Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services'* (2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final__3_.pdf>.

[173] UNICEF UK and Carnegie UK Trust, *Closing the Digital Divide for Good: An End to the Digital Exclusion of Children and Young People in the UK* (2021) <https://www.unicef.org.uk/policy/closing-the-digital-divide-uk/>.

A shift from adult definitions of privacy to reflect the needs of children is required. For instance, a uniform definition of cyber-bullying is required. Presently, confusion exists about whether this covers only singular instances or repeated occurrences. Similarly, there is uncertainty about whether cyber-by standing involve users who directly witness cyber-bullying or when users have heard about or are aware of the incidents.[174] There is a lack of consensus on its definition in conducting CRIA. Given the absence of a legal mandate, it is not viewed as a priority. The further absence of evidence of its effective results in an insufficient understanding of its advantages. Being overly bureaucratic and having methodological difficulties in disaggregating children into different groups constitute some practical challenges.[175] Clearer definitions are a sine-qua-non for an expansive reading of data protection laws and policies.

(b) Revised enforcement mechanisms

Stronger enforcement regimes are needed in general. Hardening regulation of online services in the garb of online safety must be discouraged to bolster practice codes like the AADC. Presently, the AADC pursues a risk-based approach and adds age-verification systems as a recommended feature. While the AADC recommends obtaining as little information as possible about children, lawmakers in the UK are leaning towards preventing the use of end-to-end encryption. Monitoring for protection through age-verification checks must not lead to potential profiling. While the ICO can issue penalty notices of up to GBP 17.5 million/ 4 % of worldwide annual turnover for enforcement, reform is needed in the goals that the AADC seeks to achieve.[176] Worse still, Section 125(4) of the UK DPA categorically shields non-compliance from legal proceedings. The largely recommendation-based regime may be ineffectual in bringing about significant change in data protection policies of internet platforms. Effectively enforcing the AADC requires a change in approach. Technical measures to place self-certification upon users will help.

[174] Stoilova, Livingstone and Khazbak (n 127) 33, 42.
[175] Livingstone, Mukherjee and Pothong (n 70).
[176] Natasha Lomas, 'UK Now Expects Compliance with Children's Privacy Design Code', *TechCrunch* (2 September 2021) <https://social.techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/>.

Moreover, age-gating systems/methods can help prevent access to children under a certain age. All included organisations should mandatorily conduct impact assessments to impose safeguards depending on the potential risks of harm. Tailored user experiences based on child-friendly disclosures can help in that regard. While the AADC is largely recommendation-based, certain non-negotiable practices ought to be framed in an authoritarian manner.[177] To improve enforcement of the AADC, six key challenges need to be addressed – (i) balancing protection and participation, (ii) determining age-appropriateness by reference to substantial differences within age groups of children, (iii) more guidance through criteria/standards for age-verification systems, (iv) greater parental responsibility without affecting the child's digital independence, (v) trans-national regulation to include non-UK companies whose potentially harmful content nonetheless reaches children in the UK, and (vi) developing media literacy for children to understand how data is created and used.[178]

The Metropolitan Police Service Gangs Violence Matrix poses an unacceptable risk unless it complies with domestic and international instruments on data protection. Robust data sharing agreements with government agencies and local authorities should be in place for clear guidance on data retention and processing. This approach can also reform children's data usage in algorithm policing.

(c) Technical solutions

One technical solution to the gaps in the protection of children from exploitation is to conduct regular rights-impact assessments. This will help protect the best interests of the child and help involve children when considering the range of rights to be protected. When looking at children of different age groups with different maturity levels, their evolving capacities can then be considered. In addition, privacy-by-design is crucial for default data minimisation. This default non-collection ensures that children and parents do not have to be acquainted with complex data processing technologies.

Moreover, transparency central to data processing services will ensure that users are notified of any significant changes in processing systems. Furthermore, profiling systems can be operated to automatically exclude the personal data of those under 18 years of age. This approach could, in turn, be applied even to commercial activities and business responsibilities.[179]

[177] Adele Harrison, 'The UK's Age-Appropriate Design Code in Effect', *Orrick* (26 July 2021) <https://www.orrick.com/en/Insights/2021/07/The-UKs-Age-Appropriate-Design-Code-Comes-into-Force-in-September-2021>.
[178] Livingstone (n 160).
[179] van der Hof et al (n 145).

To regulate access to sexually explicit content, age-verification systems need to be more robust to ensure that they cannot be easily bypassed. This requires cohesion across platforms and strict checks on identification documents to catch fake passwords that are illegally acquired and used to circumvent mandatory age-verification mechanisms. Sophisticated technologies need to be employed to catch usage of VPNs to bypass age-verification systems. Verification providers, including third-party providers, need to have strong privacy settings that protect personal information. Finally, a separation between verification providers and digital platforms needs to be maintained to prevent abuse of user data.[180]

Companies must take appropriate action to report content that seeks to exploit children criminally. Some steps include strict terms of service, prompt identification of inappropriate content, preventing abusive search content from appearing, strong action against live streaming of sexually illicit content and operational reporting to the appropriate authorities. Reporting options must include context that seems harmless but is harmful when seen in the relevant context. The design and development of technological systems and processes must consider this evolving landscape. Collaboration among companies to share data, tools and techniques is pivotal to combat criminal exploitation by responding to threats more effectively.[181]

Under the broad umbrella term of 'modern slavery', forced labour and marriage, debt bondage and exploitation of children have come to be identified. In fact, the Alan Turing Institute has urged that data science and machine learning methods be employed to track and prevent sexually exploitative behaviours and practices.[182]

Lastly, special protection measures are needed to protect children from sexual and economic exploitation. Another aspect worth mentioning is the need for strong age-verification systems to prevent access to harmful activities like drugs, weapons, trafficking, fraud, identity theft and even services like gambling. In addition, the state has a particularly important role in protecting more vulnerable children, such as migrant children or those who are victims of an armed conflict.

Box 13: CRIA for children in disadvantaged situations

[180] Yar (n 141).
[181] Zagaris (n 159).
[182] The Alan Turing Institute, 'Data Science for Tackling Modern Slavery', *The Alan Turing Institute* <https://www.turing.ac.uk/research/research-projects/data-science-tackling-modern-slavery>.

Child rights impact assessments can also aid in minimising discrimination by identifying the impacts on children in disadvantaged situations.[183] The kind of online risk also influences the level of vulnerability. For instance, children of LGBTQI orientation or those suffering from socio-economic precarity are more vulnerable to 'sexting'-based exploitation or victims of 'sextortion'[184]. Vulnerability also has a gendered dimension. Girls are more likely to receive sexually inappropriate content or become coerced recipients of 'sexting'. In pursuing this gap-filling function, it must be understood that online vulnerability emanates from offline circumstances. There is a need to have child protection specialists take care of vulnerable children by understanding their experiences and helping them enforce their legal rights.[185] In addition, strong end-to-end encryption policies are needed in digital communication channels without adopting an absolutist position. A balance has to be drawn to encompass situations where law enforcement authorities should be able to decrypt and analyse encrypted data for crime prevention purposes.[186]

The best way to support vulnerable children is to have a comprehensive parental support system. Comprehensive child support networks must engage in digital literacy programs and parental mediation to ensure family stability and improve skills and awareness in relation to the digital environment. In addition, support strategies must foster self-efficacy and resilience to produce a safe online environment.[187]

[183] Livingstone, Mukherjee and Pothong (n 70).

[184] It refers to threats to disseminate private images/messages or any other form of private, sexual content without consent for the purposes of exacting revenge or procuring more images, money or further sexual acts.

[185] Stoilova, Livingstone and Khazbak (n 127).

[186] Daniel Kardefelt-Winther et al, *Encryption, Privacy and Children's Right to Protection from Harm* (Innocenti Discussion Paper, 2020) <https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html>.

[187] Mariya Stoilova and Sonia Livingstone, 'Putting Children at the Centre: Is Re-Designing the Digital Environment Possible?', *Media@LSE* (20 June 2019) <https://blogs.lse.ac.uk/medialse/2019/06/20/putting-children-at-the-centre-is-re-designing-the-digital-environment-possible/> ('Putting Children at the Centre').

4 Commercial advertising and marketing

Children are repeatedly shown age-inappropriate and potentially harmful content from specifically targeted advertisements, which most disproportionally disadvantages children who are more vulnerable to manipulation. All children are at risk; however, specific reports show that young girls are more likely to be affected by content glamorising diets, body image or disordered eating. Controllers publicly mitigate the issues by claiming that more sensitive content is only shown to age-appropriate users verified by their data; however, this is simply not certain as numerous reports show otherwise. The nature of continually refreshing newsfeeds benefits the controller, given that the evidence disappears. The problem is that once a child submits their true age to create an Instagram, they are clearly told they are too young and so can resubmit a new age. Inadequate age-assurance mechanisms are the main contributor to harm.

4.1 Background

We now turn to the impact of commercial advertising and marketing and social media on children. The two phenomena are closely linked: each newsfeed on every social media site is perfectly tailored to the individual user to stimulate maximum engagement, facilitated by data collection, which is then sold to third-party advertising companies to create personalised advertisements. The average consumer is most interested in dramatic and controversial content, which means their newsfeeds are usually filled with potentially harmful and inappropriate content. Aside from this being a society-pan issue, it disproportionally disadvantages children, who are more likely to be influenced by the content they are shown, as they cannot distinguish between regular and artificially manipulated content. The algorithm works as follows: a young person is shown an Instagram account that glorifies eating disorders on their news feed. The young person clicks on the post and either engages with it (by liking, commenting, retweeting, or following the account) or moves on. Either way, the algorithm has noted that young people are interested in that *particular* content and will litter their feed with similar content to increase engagement. This includes advertising products or services that accompany that content, such as metabolism-boosting 'Skinny teas' or diet pills.

All children are at risk of being influenced by harmful content; however, research shows that young girls are more likely to be affected by content promoting diets, disordered eating, or an idealised body image. Similarly, statistics demonstrate that young girls are more likely to commit self-harm and suicide and engage more with this type of content.[188]

[188] Elizabeth M Ozer et al, *America's Adolescents: Are They Healthy?* (2003).

4.2 Digital participation and potential harm

The GC summarises digital harm in commercial advertising and marketing:

> The digital environment includes businesses that rely financially on processing personal data to target revenue-generating or paid-for content, and such processes intentionally and unintentionally affect the digital experiences of children. Many of those processes involve multiple commercial partners, creating a supply chain of commercial activity and the processing of personal data that may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content.[189]

Each newsfeed on every social media site is perfectly tailored to the individual user. The platform aims to show perfectly matched content to the user to increase engagement and collect more personal data on their likes and interests to customise the newsfeed. Recommender systems prioritise showing consumers content that will spark the greatest engagement, prioritising the most attention-grabbing topics. Unfortunately, this is a classical 'if it bleeds, it leads' scenario. The average consumer is most interested in dramatic, controversial, and scandalous content, as opposed to more mundane and everyday truths. Aside from this being a society-pan issue, it most proportionally disadvantages children, who are more likely to be influenced by the content they are shown. Different interests, likes, and behaviours are also more likely to develop in the teenage years, as the young person becomes more self-aware and fosters greater links with society. Again, care must be taken to ensure these interests do not foster into something harmful, where inappropriate content was the catalyst. Further research needs to examine the *cause* of the harm, rather than just identifying it.

For example, an algorithm might work like this: a young person is shown an Instagram account that glorifies eating disorders on their news feed. The young person hovers to view a post or scrolls past further. They may click on the post then either click away or follow that account to see more posts. Either way, the algorithm has noted that young people are interested in that content, so it will litter their feed with similar content to increase engagement.

[189] *General Comment No. 25* (n 2) 25.

The purpose of targeted advertisements is to achieve the same effect. The Elysian Fields of the digital sphere for advertisers and advertising platforms (including social media) is perfect discrimination: where advertisements distinctly match their targeted human counterparts intending to achieve a 100% conversion rate, where each click equates to a purchase made. If a young person engages with content promoting eating disorders, their newsfeed and advertisements would dually reproduce this. For example, the young person may be shown advertisements for skinny teas, diet pills, or waist trainers to encourage purchase. In this sense, a young person's data becomes a commodity. Using children's personal data for marketing includes sending marketing messages to individual children (direct marketing) and displaying targeted adverts in an online context (otherwise known as behavioural advertising).

Platform providers justify their recommender systems based on creating the best user experience; however, in reality, it serves in the best interests of the platform themselves. Targeted advertisements account for over 70% of online revenue, encouraging firms to collect more personal information to create highly tailored advertisements and achieve personal information.[190] The service providers' primary goal is to maximise targeted advertisement profit. Higher revenue provides incentives to collect more data to increase the accuracy of advertisements and ultimately collect more profit. The consequential effects of expansive data collection are more efficient platforms that suit consumer needs, identified by processing. The result is increased engagement with their platform and more visibility for the advertisements, which increases profit generated by targeted ads and entrenched market power from the possession of data. This creates a 'lifecycle' of inappropriate content:

[190] Competition & Markets Authority, *Online Platforms and Digital Advertising* (2020).

Figure 1: Recommender systems create lifecycle of inappropriate content and advertising

These issues are heightened in a digital environment where newsfeeds are phantasmic: once refreshed, the previous content disappears and is untraceable. By comparison, magazines remain accountable, where an adult or parent can verify the content before passing it to the young person. Unfortunately, a similar standard of accountability or verification cannot be duplicated in the digital space.

4.3 Child rights opportunities and impacts

(a) Non-discrimination

The GC outlines that "States parties ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them."[191] In brief, the ambition is to overcome digital exclusion. Children are protected against all forms of discrimination based on status, activities, race, colour, sex, language, religion, political or national, ethnic or social origin, property, disability, birth, or another status. A child's digital profile could potentially contravene this article. An online identity is created based on assumptions made from the child's usage and interaction with certain content in the digital space, which may not accurately reflect their true nature or character. For example, a child may dabble in violent content or accidentally engage with accounts that promote hate or racism. These attributes then become part of the child's 'digital profile' to aid the algorithm in matching similar content to maximise engagement. As a child develops online, they are likely to make harmless mistakes, engage in unwanted content that does not accurately reflect their world views, and change their opinions as they grow. However, alternations are not permitted in the digital environment. Once you are identified as a user interested in violence, it is set in stone. There is no backspace or delete when it comes to data collection, hence policy concerns that there is no real 'right to be forgotten. 'In this sense, the child can be discriminated against as their digital profile may not reflect their true character or person. Additional discrimination may arise as children are subjected to certain 'stereotype' content that they are likely to engage with. For example, females may be shown more 'body image' content and shown a range of e-commerce advertisements, such as diet products, waist trainers or even clothing. On the other hand, males may be shown sports, gaming, and even more violent content.

[191] *General Comment No. 25* (n 2) 3 [9].

(b) Best interests of the child

The digital environment was not originally designed for children, yet it plays a significant role in their lives. Hence, all actions concerning children should be in the child's best interests as a primary consideration extending to the actions of public or private social welfare institutions, courts of law, administrative authorities, and legislative bodies. The GC provides that "in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration."[192] The actions of the private sector are not in the best interests of the child. It becomes apparent in this report that the provider's best interests are to increase revenue from targeted advertisements without adequate safeguarding for children.

Box 14: Inappropriate content shown to young people

Although platforms have mitigated the issues by claiming more sensitive content is only to shown to age-appropriate users that is verified by their data, this is not true in practice. Previous research has shown that 1 in 5 advertisements that young children are exposed to is age-inappropriate.[193] For example, a scathing report from Common Sense researchers looked at a total of 1,600 videos viewed by children under the age of eight on YouTube Kids. The study found that ads were present on 95% of the videos watched. A fifth of the ads were deemed age-inappropriate; most notable, one advertised bourbon and the other about deporting illegal immigrants from the U.S. Only 5% of the videos had educational value. In comparison, 30% contained 'mild' physical violence, and only 24% showcased a diverse representation of race and gender. Moreover, 45% (almost half) of the videos advertised products.[194]

[192] *General Comment No. 25 on Children's Rights in Relation to the Digital Environment 2021* (CRC/C/GC/25) 3 [12] ('*General Comment No. 25*').

[193] Miranda Hester, 'How Often Are Kids Exposed to Age-Inappropriate Ads?', *Contemporary Pediatrics* (24 May 2021) <https://www.contemporarypediatrics.com/view/how-often-are-kids-exposed-to-age-inappropriate-ads->.

[194] Ibid.

Similarly, a Wall Street Journal investigation into TikTok found that a 13-year-old user could search the Only Fans subscription social platform and watch a handful of videos, including two selling pornography.[195] The same teenage user was then shown a series of sexually-oriented videos. The more the user lingered on sexual content, the more sexual content was shown in the 'for you page,' regardless of the user's age as part of their profile. In a further study, one account registered as a 13-year-old was shown at least 569 videos about drug use, with references to cocaine, meth addiction, and promotional videos of online sales and drug products.[196] The defining nature of TikTok is an endless supply of short, 20-second, attention-grabbing videos, meaning that young people are exposed to masses amount of content in a short space of time. Imagine the harm imposed when children use these sites for several hours per day. In response to these alarming studies, a TikTok spokeswoman said that the app does not differentiate between videos it serves to adults and minors but said that the platform is looking to create a tool that filers content for young users.[197]

(c) Right to life, survival and development

Children have the inherent right to life and for States to ensure the survival and development of the child.[198] The GC explains the "increasingly crucial role in children's development [of the digital environment which] may be vital for children's life and survival, especially in situations of crisis."[199] For example, there are risks associated with "violent and sexual content, cyberaggression and harassment", and State parties should "take all appropriate measures to protect children from risks to their right to life, survival and development".[200] Section (d) addresses the risk of harm related to disordered eating, self-harm, suicide and other violent and sexual content shown to children online.

(d) Health and welfare

The GC provides:

States parties should encourage digital technologies to promote healthy lifestyles, including physical and social activity.[201] They should regulate targeted or age-inappropriate advertising, marketing and other relevant digital services to prevent children's exposure to the promotion of unhealthy products, including certain food and beverages, alcohol, drugs and tobacco and other nicotine

[195] Rob Barry et al, 'How TikTok Serves Up Sex and Drug Videos to Minors - WSJ' (8 September 2021) <https://www.wsj.com/articles/tiktok-algorithm-sex-drugs-minors-11631052944>.
[196] Ibid.
[197] Ibid.
[198] *CRC* (n 1) art 6.
[199] *General Comment No. 25* (n 2) 4 [14].
[200] Ibid.
[201] *General Comment No. 17 on the Right of the Child to Rest, Leisure, Play, Recreational Activities, Cultural Life and the Arts (Art. 31) 2013* 17.

products.[202] Such regulations relating to the digital environment should be compatible and keep pace with regulations in the offline environment.[203]

Children cannot distinguish between artificially manipulated or recommended content, meaning they are particularly negatively affected by commercial advertising and marketing. The digital environment includes "gender-stereotyped, discriminatory, racist, violent, pornographic and exploitative information, as well as false narratives, misinformation and disinformation", which comes from multiple sources such as "commercial content creators, sexual offenders or armed groups designated as terrorist or violent extremist."[204]

Children account for an estimated one in three internet users worldwide,[205] and growing evidence suggests that children access the digital environment at increasingly younger ages. Children under 15 are as likely to use the internet as adults over 25.[206] This stems from a 'bedroom culture,' where children prefer to interact online than in person, which the Covid-19 pandemic has only exacerbated. Restrictions and stay-at-home orders saw a 50-70% increase in internet usage, where 50% of that time was spent engaging on social media.[207] Statistics suggest that the average child spends approximately six to seven hours per day on social media.[208] It is important to show that this figure only reflects social media and not an average *screen time*, where news websites, online shopping, emails, and online gaming are often neglected from empirical studies, yet where children still receive targeted advertisements. Therefore, a young person likely has much more exposure to manipulated content than statistics show.

---

[202] *General Comment No. 15 on the Right of the Child to the Enjoyment of the Highest Attainable Standard of Health (Art. 24) 2013* 15 [77].

[203] *General Comment No. 25* (n 192) 17 [97].

[204] Ibid 10 [54].

[205] UNICEF, *Children in a Digital World: The State of the World's Children* (2017) 3.

[206] Ibid.

[207] Mark Beech, 'COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal', *Forbes* (25 March 2020) <https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/>.

[208] Jane D Brown and Elizabeth M Witherspoon, 'The Mass Media and American Adolescents' Health' (2002) 31(6, Supplement) *Journal of Adolescent Health* 153.

The digital environment exacerbates health challenges that are linked to visual influence, such as eating disorders. Beat Eating Disorder Charity has conducted research that shows 1.25 million in the UK are affected by an eating disorder,[209] where the average age of onset for anorexia nervosa is 16-17.[210] However, there is also evidence of eating disorders developing much younger than children as young as six years old in the most extreme cases. Young people between the ages of 14 and 25 have been identified as most at risk.[211] Males make up 25% of those affected by an eating disorder, and females and non-binary people make up 75% of cases.[212]

The digital environment (most especially social media) is a significant contributor to the increase in poor body image and eating disorder cases. An endless cycle of appeasing and ‘perfect ’content gives rise to a certain body type that matches the modern idealised standards of beauty and attractiveness in western society. Over time, the idealised cultural body has become leaner and thinner for females and bigger, taller, and muscular for men. In a time of ‘diet culture,’ Instagram and Tumblr are leaders in glorifying disordered eating and calorie counting, all easily found under the hashtag ‘Ana, ’a term coined for the disorder. A simple search with the hashtag #ana brings up endless harmful content, where users either document their struggles or form support networks to encourage other users to ‘stay strong’ and skip meals. Similarly, ads make assumptions about interests by relying on stereotypes, focusing on body image, objectification and sexualisation. Repeatedly presenting a narrow beauty ideal or body type leaves no room for diversity.

Box 15: Body image and social media

[209] ‘Statistics for Journalists’, *Beat Eating Disorders* <https://www.beateatingdisorders.org.uk/media-centre/eating-disorder-statistics/>.
[210] ‘Eating Disorder Statistics’, *Priory Group* <http://www.priorygroup.com/eating-disorders/eating-disorder-statistics>.
[211] ‘Eating Disorders - TalkED’, *Anorexia and Bulimia Care* (2 December 2021) <https://www.talk-ed.org.uk/eating-disorders/>.
[212] Ibid.

Research has shown that young people frequently report body dissatisfaction compared with the average adult, which is likely to trigger content surrounding body image. A cycle of visualisation and inappropriate content is expected to lead to disordered eating. Research has shown that adolescent girls experience more body image dissatisfaction than boys. An analysis of 25 female subjects felt negative about their body image after viewing media images of thin models. In one study, 44% of adolescent girls expressed they were overweight, and 60% were actively trying to lose weight, despite the majority being a normal, healthy weight.[213] Relevantly, a study involving sixteen-year-old girls established that the intense pressure to be thin arose from the digital space. All girls articulated a desire to be thinner, despite not necessarily being dissatisfied with their bodies,[214] demonstrating that it is an artificially manipulated general truth in light of social media promoting weight loss.

An equally alarming and problematic serious harm imposed on young children is the risk of self-harm and suicide. YouTube Kids, designed as a safer, child-friend platform that expressly operates for users under the age of thirteen, has been criticised for showing cartoons that contained clips on the different ways to commit suicide. In a sadistic twist, an energetic cartoon character designed for children attracts the targeted audience, only a man to appear in the frame, demonstrating how to cut wrists four minutes into the clip. Researchers found that posts with hashtags related to self-injury rose from between 58,000 to 68,000 in 2018 to more than 110,000 in December. A study for the International Journal for the Advancement of Counselling found that more than 1.2 million Instagram posts over the incubator period contained one of five popular hashtags related to self-injury: #cutting, #selfharm, #selfharmmm, #hatemyself, and #selfharmawareness. Moreover, considering Instagram's censorship, users and young people can easily find workarounds to avoid infringing the policies, demonstrating Instagram's feeble attempts to safeguard. For example, by purposely misspelling 'self-harm' in a hashtag with the edition of a few extra letters to create 'selharmmm', which resulted in a plethora of graphic images.[215]

Children are exposed to harmful behaviours online and then engage in the practice themselves.[216] For example, the Samaritans reported that children as young as 12 had accessed suicide and self-harm material online.[217]

[213] Ozer et al (n 188).
[214] M Tiggemann, M Gardiner and A Slater, '"I Would Rather Be Size 10 than Have Straight A's": A Focus Group Study of Adolescent Girls' Wish to Be Thinner' (2000) 23(6) *Journal of Adolescence* 645 ('I Would Rather Be Size 10 than Have Straight A's').
[215] Leigh Beeson, 'Adolescents Use Social Media to Post about Self-Injury', *UGA Today* (10 November 2021) <https://news.uga.edu/adolescents-are-posting-about-self-injury-on-social-media/>.
[216] Ibid.
[217] *Written Evidence Submitted by the Samaritans (OSB0182)* (24 September 2021) <https://committees.parliament.uk/writtenevidence/39529/html>.

Box 16: Netflix and suicide rates

A most recent example of the real-world effects of content seen online is the popular Netflix show '13 Reasons Why', which is about a schoolgirl who, before her death, recorded cassettes that detail 13 reasons why she took her own life. Given the nature of the causal connection, it is difficult to establish a link between the show and suicide rates. However, a study from the Disease Control and Prevention on suicide rates found that in April 2017, the month in which the show premiered, rates increased by 29.9% among youths in the US between 10 and 17 years old. The study estimates that the spike was responsible for about 195 "extra" deaths by suicide between April and December 2017, beyond the existing trends suggested.[218] In another study, 21 out of 43 participants of young adults who had watched the show said it heightened their suicide risk.[219] Where April 2017 saw a 29.9% increase in suicide rates alongside the premiere of '13 Reasons Why,' boys mostly drove the spike, and the shift among girls was not statistically significant.[220] Validity of the study aside, the main concern is that accessibility to content that glorifies self-harm undoubtedly influences young, impressionable users. They may seek 'fame 'after death as in the Netflix show to gain acceptance to online forums, to interact and seek friendship online, or become accustomed and desensitised to harmful acts that may be considered 'normal' given that others are doing it.

[218] Catherine Saint Louis, 'For Families of Teens at Suicide Risk, "13 Reasons" Raises Concerns', *The New York Times* (online, 1 May 2017) <https://www.nytimes.com/2017/05/01/well/family/for-families-of-teens-at-suicide-risk-13-reasons-triggers-concerns.html>.

[219] Beata Mostafavi, 'Does Netflix's "13 Reasons Why" Influence Teen Suicide? Survey Asks At-Risk Youths', *Michigan Health Lab* (20 November 2018) <https://labblog.uofmhealth.org/rounds/does-netflixs-13-reasons-why-influence-teen-suicide-survey-asks-at-risk-youths>.

[220] Constance Grady, 'Netflix's 13 Reasons Why Linked to a Spike in the Youth Suicide Rate', *Vox* (online, 3 May 2019) <https://www.vox.com/culture/2019/5/3/18522559/13-reasons-why-netflix-youth-suicide-rate>.

A recent trend in the data shows an increasing number of young boys committing suicide and self-harm. The rate of self-harm among young children has doubled over the last six years, where the number of children aged nine to twelve admitted to hospital from self-harm rose from 221 in 2013 to 508 in 2020. This equates to an average of ten hospital admissions every week within this age bracket, where the true picture of those over twelve is much higher.[221] Suicide rates among young people are rising in general, reaching the highest levels since 2000, which saw a 21% rise in boys aged 15-19 dying by suicide in 2017 from the year before.[222]

Adolescence is a vulnerable time. Exposure to inappropriate content, particularly of a violent or self-injuring nature, can foster disassociation and comfortability with illegal or harmful actions. All harmful content negatively disproportionately affects young people more than society at large. However, young females and non-binary are more at risk of disorders and self-harm, which means they are likely to be more influenced by harmful content. This is especially true as females engage more on average in manipulated content and targeted advertisements by males.

(e) Civil rights and freedoms

Freedom of expression

Freedom of expression permits the child to seek, receive and impart information and ideas on any media. Children have reported that the digital environment offers 'significant scope to express their ideas, opinions and political views.' [223] The idea is that children should be shown information from a large diversity of ideas, particularly from minority sources or under-represented groups to help develop a sense of self and decide for themselves on how to express those ideas. However, a perfectly-tailored algorithm impedes diversified access to information. The algorithm will continue to show the child content and ideas that the child has previously shown an interest to optimise engagement. The algorithm will not introduce new, minority content that has the risk of disengaging the user. Therefore, the child is presented with glossy, superficial content that may not be representative of all society or even demonstrates a holistic account of the idea. This is particularly dangerous for minority children who may be shown 'popular' content that does not represent their culture of heritage.

[221] Sarah Marsh, 'Self-Harm among Young Children in UK Doubles in Six Years | Mental Health | The Guardian', *The Guardian* (16 February 2021) <https://www.theguardian.com/society/2021/feb/16/self-harm-among-young-children-in-uk-doubles-in-six-years>.
[222] Alia Dastagir, 'Youth Suicide Rate Increased Dramatically in Last Decade, CDC Says', *USA Today* (11 September 2020) <https://www.usatoday.com/story/news/health/2020/09/11/youth-suicide-rate-increases-cdc-report-finds/3463549001/>.
[223] *General Comment No. 25* (n 2) 10.

Freedom of thought, belief and religion

Companies identify and exploit people's or communities' behavioural patterns and characteristics through targeted advertising. The content shown on social media is proven to be highly influential. The impacts of fake news, diminishing truth online, and limitations on freedom of thought is a society-pan issue. It also specifically disadvantages children who have not had the life experience and maturity to develop their independent thoughts and opinions. Instead, they are bombarded with artificially manipulated content, resulting in inappropriate interests and behaviours that would not have arisen if not for exposure to the content. Surveillance-based advertisement has significantly contributed to the exploitation of children's particular characteristics to increase the persuasiveness of advertising, thereby unjustifiably interfering with their absolute freedom to form an opinion and enjoy independent thought processes. Children using platforms' services are being manipulated to think or make decisions they would have otherwise never made.[224] Special protections against surveillance-based advertising should be considered for vulnerable groups, such as children and young people.[225]

Right to privacy

No child should be subject to arbitrary or unlawful interferences with their privacy.[226] 'Opt-in' by default to cookie-based tracking without true consent or understanding encroaches on a young person's privacy, especially when the data is subsequently shared with third parties to create advertisements. A young person has no idea that data is being collected about them, shared, and then used to create a manipulated environment to retain their interest and engagement. Moreover, children are unlikely to fully understand the terms of service or what information disclosure, meaning that their willingness to pay with their data in exchange for the use of the platform is not proper consent.

[224] Holli Sargeant, Julia Haas and Eliska Pirkova, 'AI in Content Curation and Surveillance-Based Advertising' in Julia Haas and Deniz Wagner (eds), *Spotlight on Artificial Intelligence and Freedom of Expression: A Policy Manual* (OSCE, 2022) 80 <https://www.osce.org/representative-on-freedom-of-media/510332> ('Spotlight on Artificial Intelligence and Freedom of Expression').
[225] Ibid 94.
[226] *CRC* (n 1) art 16.

(f) Protection from economic, sexual and other forms of exploitation

Children are exploited for economic gain from targeted advertisements, where the inappropriate content is directly harmful to their physical, mental, and social development. A child's right to protection against economic exploitation is contained in Article 32 UNCRC:

> the right to be protected 'from economic exploitation and from performing any work that is likely to be hazardous or interfere with the child's education.' Although usually understood as protection against child labour, the right needs to be reconfigured in the digital environment to protect children against a mosaic of economically exploitative methods.

Economic means a material interest or profit, while 'exploitation' is defined as 'taking unjust advantage of another for one's own advantage or benefit.'[227] Complex revenue models behind newsfeeds and user interfaces (the material interest) collect children's data to input into algorithms that profile the child. Personalised advertisements are created from those profiles that nudge the child to buy products or even in-app items to advance in games (manipulation).

Originally coined by UX specialist Harry Brignull, dark patterns are user interfaces that have been specifically designed to trick users into certain behaviours, such as signing up for recurring bills or purchasing through advertisements.[228] Service providers use these interfaces to fraudulently manipulate children into behaviour that benefits the company. For example, limitless newsfeeds encourage users to scroll continuously or 'accept' buttons are placed at the top of a terms and conditions page rather than at the bottom, which the user would have to scroll through and read. Personalised advertisements are targeted using a digital profile to encourage purchase. Service providers use 'dark patterns' to manipulate children with fraudulent interfaces that are designed to mislead the user.

Children's data can be exploited multiple times and by numerous parties. A website can sell behavioural data of a child to the highest bidder during real-time bidding, from which the bidder can interpret for advertisement to persuade the child to buy a certain product. These two examples of exploration demonstrate an indeterminate liability to an indeterminate amount.

The Council of Europe adopted guidelines to protect children against economic exploitation:

---

[227] Committee on the Rights of the Child, *UNCRC General Day of Discussion 1993, Economic Exploitation of Children* (No UN Doc CRC/C/20, 1993).

[228] Arvind Narayanan et al, 'Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces' (2020) 18(2) *Queue* 67 <https://dl.acm.org/doi/10.1145/3400899.3400901> ('Dark Patterns').

> "States should take measures to ensure that children are protected from commercial exploitation in the digital environment, including exposure to age-inappropriate forms of advertising and marketing. This includes ensuring that business enterprises do not engage in unfair commercial practices towards children, requiring that digital advertising and marketing towards children is clearly distinguishable to them as such, and requiring all relevant stakeholders to limit the processing of children's personal data for commercial purposes."[229]

As previously discussed, children are repeatedly shown age-inappropriate content due to insufficient safeguards and the inability (or feeble attempt) to establish age assurance with certainty. The commercial practices are directly harmful to the child's physical, mental and social development.

4.4 General measures of implementation by States parties

(a) Legislation

Children face challenges in access to justice relating to the digital environment because there is a 'lack of legislation placing sanctions on children's rights violations specifically in relation to the digital environment, … difficulties in obtaining evidence or identifying perpetrators or because children and their parents or caregivers lack knowledge of their rights or of what constitutes a violation or abuse of their rights in the digital environment.'[230]

Data Protection Framework

Platforms offering advertising services must comply with the Data Protection Act 2018 (**DPA**), the UK implementation of the General Data Protection Regulation (**GDPR**) and, in some cases, the Privacy and Electronic Communications Regulations 2003 (**PECR**). Some kinds of online advertising may arguably constitute 'direct marketing' under PECR – particularly where advertisers target known individuals from their contact lists through digital advertising systems or where individuals are targeted based on some unique combination of demographic characteristics and predicted interests. Still, most forms of online targeting would not fall within PECR's requirements to obtain consent to send direct marketing via email. Children are also afforded special protection under DPA and GDPR.

[229] Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Recommendation CM/REC(2018)7 of the Committee of Ministers) 20.
[230] *General Comment No. 25* (n 2) 8.

AADC

The Age-Appropriate Design Code (**AADC**) provides recommendations for the design of platforms to minimise harm to children.[231] This is a statutory code of practice prepared under section 123 of the DPA. In accordance with section 127 of the DPA, the Commissioner must take the code into account when considering whether an online service has complied with its data protection obligations under the GDPR or PECR. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the GDPR. The AADC is not itself justiciable; however, where there is another relevant cause of action, the AADC will support and add depth to an argument in respect of online harm to children. The preamble to the AADC clarifies that it can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant.[232]

(b) Comprehensive policy and strategy

The Online Safety Draft Bill shows considerable progress in this space. In particular, its references to "children in different age groups". The House of Lords and the House of Commons provided a pre-legislative report of the Online Safety Draft Bill. The Online Safety Draft Bill aligns with the AADC, but seeks to demands further, statutory change, such as regulation of rules for age assurance. This is undoubtedly a step in the right direction and has the dual potential to capture more harm and align with the actual capabilities of children's intellectual abilities and understanding.

There is no regulatory code in the UK that sets out rules for age assurance. The Online Safety Draft Bill outlines that current proposals cannot be properly implemented without a statutory system of regulation of age assurance. Hence, there is a gaping hole in the regulatory framework that is well established and well reported.[233]

Furthermore, The Online Safety Bill recognises that there ought to be a specific responsibility on service providers to identify reasonably foreseeable risks of harm arising from the design of their platforms and take proportionate steps to mitigate those risks of harm.[234] To achieve this, a recommendation of this report is that the Draft Bill should set out a non-exhaustive list of design features and risks associated with them to provide clarity to service providers.

[231] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58).
[232] Ibid.
[233] *Draft Online Safety Bill* (n 149) [227] Section 5 Protection of Children.
[234] *Ibid Section 5 Protection of Children.*

4.5 Gaps in current frameworks

The legislative framework neither obtains legitimate consent, coherently explains when a DPIA should be undertaken, nor provides statutory rules of age assurance. The former is a society-pan issue that has substantiated much of the critique of GDPR, but the second issue directly affects children's use of the digital environment. The AADC has attempted to fill this gap by encouraging platforms to confirm the age of the user 'by-design.' The quality of the recommendations aside, the content of the code is not enforceable and, therefore, by default, falls short of practical and effective implementation.

(a) Consent

The DPA set out six possible lawful bases for data processing. Social media platforms appear to rely on a combination of contract, consent, and legitimate interests as its lawful basis for data collection for its advertising system. Consent is often relied on in relation to processing children's personal data, although evidence shows it is often not freely given nor informed.[235]

Consent is an overarching issue with GDPR. Calculated design choices coax consent to cookie-based tracking, where an 'opt-in' is the default. The two models that websites use to abide by GDPR are the *implied consent mechanism* and a *forced opt-in*. The former is where the user must agree to the use of cookies if they continue to use the website, and the latter incorporates a banner notice that prevents the user from accessing the site unless the use of cookies is confirmed. A similarity between the two models is that the user is blocked from accessing the content unless they consent. In addition, agreeing to terms of service is sometimes presented in bold, larger front, where one may have to scroll to find the rejection.

Moreover, consent by default appeals to present bias, where consumers cannot read lengthy terms of service or do not understand why they need to. There is a plausible partial vindication that adults may refer to the terms of services, yet this cannot be extended to children, who should neither be expected to seek out the information nor comprehend its contents. Therefore, a lack of consent is an expansive issue that specifically disadvantages children.

[235] *GDPR* (n 55) article 7, 8.

The reality is that young people can access TikTok and all the harmful content featured on the platform because no real safeguards are preventing them from doing so. TikTok's terms of service say that users must be at least 13 years old and that users under 18 need consent from their parents. Terms of Service notoriously protect the platform from legal liability rather than safeguarding the consumer. If the average adult consumer does not read terms and conditions or terms of service, the average child certainty won't, nor are they in a position to understand the content.

The AADC outlines that platforms should present privacy information "in clear language suited to the age of the child" [236] to obtain consent and promote transparency.[237] 'Bite-sized' explanations are proposed as a safeguarding measure. This is in accordance with the requirement under 5(1) of the GDPR to process personal data: 'lawfully, fairly and in a transparent manner in relation to the data subject.' Although seemingly promising, the AADC dictates that the information should be "easy to find and accessible for children."[238] Given that the average child is too young to understand data, information, or even privacy as a general concept, it is unrealistic to believe they would be naturally interested in these topics. Let alone nor attempt to *find* it in platforms specifically designed to capture and retain their attention elsewhere.

Additionally, the AADC recommends that bite-sized explanations pop up at the point at which the use of personal data is activated. A fleeting, one-time message will certainly not create a lasting impression on the child or facilitate their understanding, especially when they are driven by a desire to access the same content that the pop-up blocks. The following is an example of an ICO-approved notification:

[236] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 37.
[237] Ibid.
[238] Ibid.

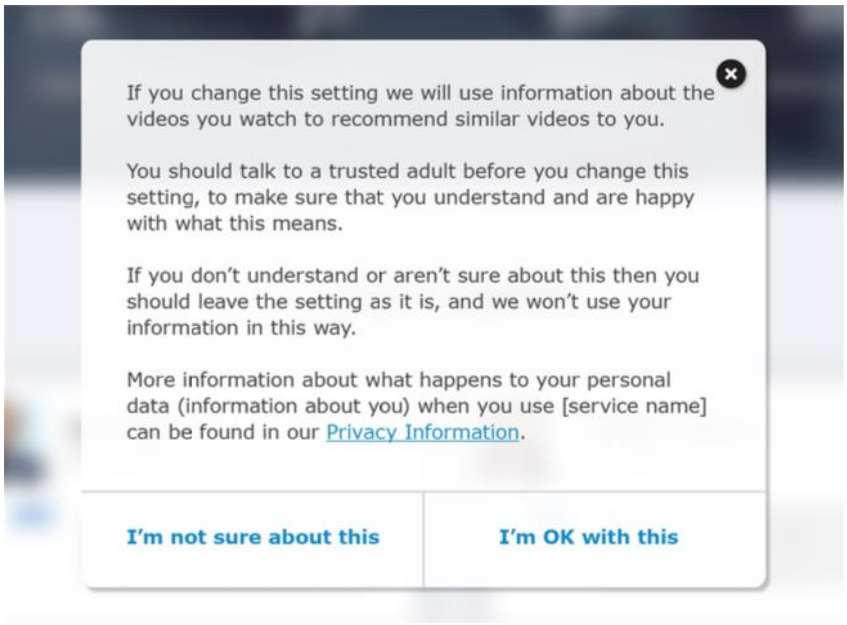

Figure 2: An example of a clear, bite-sized example taken from the Age-Appropriate Design Code to notify children on how their data is used.[239]

The above notification will not appeal to a child. Out of context, an onlooker would assume the notification is tailored for a regular, adult user. The text is dense, unappealing, and is not designed to specifically highlight the most important aspect of the notice: *If you watch this video, we will recommend similar videos to you.* The average child will not pick out this as the most crucial line in the banner. The example completely lacks any considerations of educational psychology, especially in the context of children. Primary colours, pictures, and bold texts all have the potential to convey a message to a child accurately. The above example packs lots of information into one notice and certainly does not constitute 'bite-sized'. The result is that poor recommendations are given to platforms on effectively conveying information to children.

[239] Age-Appropriate Design Code, 38

The AADC is accompanied by different age brackets from 0-5 years to primary school, transition years, early teens and approaching adulthood. The AADC recognises that a one-size-fits-all approach is not appropriate, given that children have different needs at different stages of their development. There are positive aspects of the recommendations, including clear signposts of what information a child needs to know: the basic concepts of online privacy, privacy settings, who can see what, their information rights, how to be in control of their information, and respecting other people's privacy. Moreover, cartoon, video, or audio materials are heavily recommended and repeated. However, there is one glaring and inappropriate default. In the age 0-5 bracket, which is described as 'pre-literate & early literacy', upon attempting to change their privacy settings, the child should be met with a prompt to leave things as they are or seek help from a parent before changing their settings. This remains true for 6-9 years and 10-12 years brackets. The issue is simple: children who are 'pre-literate' or soon after should *not* be permitted to change their privacy settings, regardless of the 'advice 'that pops up. This is because the child will fundamentally not understand the consequences of their actions nor be able to property read the pop-up, therefore invalidating any 'consent' given.

(b) Age assurance

Platforms need to identify the age of their users to tailor age-appropriate content and ensure they are appropriate for their use and developmental needs.[240] The AADC provides only two examples of design features that discourage false declarations of age or identity: neutral presentation of age declaration screens (to deter nudging towards certain ages) and preventing users from immediately resubmitting a new age if they are denied access when they first self-declare their age. Although these measures sound positive, they are inadequate in practice. Firstly, they are not prescriptive enough: users should be prevented from immediately resubmitting a new age. Immediately is a subjective notion. What is the benefit of stopping a child from immediately gaining access when they can in the next five minutes or in a few days? The child is likely only to make the mistake of giving a true age once; therefore, it is unlikely to be repeated when signing up for the plethora of social media accounts available. Most crucially, social media platforms are simply not following the recommendations. For example, one may immediately resubmit their age on Instagram when initially denied access. The AADC recommendations should go further to provide instructions.

[240] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 32.

The AADC presents self-declarations of age as a design feature to determine user age, although not a stand-alone solution. A declaration is an inadequate tool to ensure privacy protection for children. It completely disregards all behavioural economic considerations (present biases, a predisposition for short-term benefit) and will not deter children from accessing inappropriate information. This will drive a lifetime of unsuitable targeted advertising due to the cookies collected and data profiling. This is indeed a 'lifetime' issue. Consumers have limited powers to access their data and rectify their data, so the content they have previously accessed will remain attached to their digital identity for an unknown period of time. The AADC is not prescriptive enough to be fully informative or applied uniformly. For example, why does the report not offer a series of vetted third-party services? Is it most effective for the burden of authenticating these services to fall on the platforms? How *exactly* can AI be used to determine age? The recommendations seem to raise more questions than solutions, which will certainly be overlooked in light of their non-enforceable nature.

Clarification is needed on the status of liability and potential negligence in failing to age authenticate the user, the advertisements, and the content generated by a recommender system.[241]

(c) DPAI

A Data Protection Impact Assessment (**DPIA**) under the GDPR is an assessment of the platform that online providers must undertake to identify and minimise the data protection risks of their service. They are especially important if there are specific risks to children who are likely to use their service. There is no specific statutory requirement of when to complete a DPIA, but GDPR recommends that they are conducted before any type of processing that is likely to result in high risk.[242] If the DPIA is completed before the service is launched, then it ensures the outcomes can influence the design.[243] There are two main prima facie issues with this statement. First, the DPIA must be conducted *before* processing, therefore not casting a wide enough net for the infringing platforms *already* processing and have achieved a dominant market share (such as TikTok, YouTube, Facebook, all of which have been previously discussed). These are the platforms that are committing the most harm.

[241] To further expand on this, for example, Children's Commissioner, *Life in Likes: Children's Commissioner Report into Social Media Use among 8-12 Year Olds* (4 January 2018) <https://www.childrenscommissioner.gov.uk/report/life-in-likes/>.

[242] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 27.

[243] Ibid 28.

Second, the fault lies in the statement of 'high risk,' which gives no specific definition or instruction. Even so, platforms are given an exceptionally vast threshold for what may constitute a 'risk' which seems particularly archaic given the advancements in competition laws towards foreseeable or likely or potential risks. GDPR seems to give an unusually high threshold for harm, which is disproportional to the surrounding competitive and legal landscape. There is no justification to provide the platforms that are committing the harm with even more discretion to commit further harm.

DPIAs dictate that if a website processes a vulnerable person's data (such as children) and there is a 'high risk' of harm, the provider should conduct a risk assessment that specifies how design features and processing seek to deter harm. The issues raised are two-fold: there is a high threshold before completing a risk assessment, and there is no definition for what constitutes a 'harm.' This lethal combination will result in harmful practice slipping through the net and DPIAs being neglected. It is especially inadequate (and archaic) as the status quo of foreseeability of risk in the competitive landscape is substantial and even moving towards likely in recent times. Another issue is that it is 'good practice' to publish DPIAs to promote transparency, not a requirement.

Even wider discretion is permitted in step 3 of the DPIA: consulting with children and parents. Platforms *can* seek the views of parents to 'take them into account in [their] design.' The ICO' expect(s) larger organisations to do some form of consultation in most cases.' The language used in the AADC allows broad discretion to the platforms to decide whether they wish to seek advice from the public and essentially gives them a non-enforceable option. The provision of a workaround emphasises this: if the platform considers that "it is not possible to do any form of consultation, or it is unnecessary or wholly disproportionate, [they] should record that decision in your DPIA" where they later may have to justify their decision.[244] The lack of enforceability leaves a huge vacancy of potentially very insightful feedback and information to mitigate online harms for children. For example, market research could feedback the child's ability to understand terms and conditions or how the platform uses their data.

Step 5 and 6 of the DPIA instructs the platform to 'consider' whether any changes can be made to "reduce or avoid each of the risks" identified. The flexibility of the language of the DPIA reflects both its lack of authority and effectiveness. It seems to disproportionally benefit online providers by mitigating some of the required steps in the DPIA by providing workarounds or considerations, as opposed to specific analysis. The AADC indeed requires platforms to implement the measures in the report; however, when the measures are inadequate safeguards and dually allow the platform's discretion, the requirement is not very convincing.

[244] Ibid 29.

DPIAs grant service providers with a magnitude of discretion in compliance. However, service providers appear to capitalise on the flexibility in collecting non-essential cookies by claiming that it is 'in the legitimate interests of the company,'[245] an exception granted under GDPR. Whether the cookies collected are in the interests of the company or whether it is a façade to collect as many cookies as possible is a grey area. The ambiguity is only execrated by the broadness of 'legitimate interests of the company,'[246] which includes direct marketing and research and development. The all-encompassing nature of these categories begs the question what data *wouldn't* fall under these categories. Therefore, granting provides with discretion under DPIAs is likely to only result in minimum compliance alongside maximum data collection. Although the Code envisages individual firm-centric data standards and regimes, perhaps a one-size-fits all approach is the only effective method, despite potentially innovation-stifling.

(d) Enforceable regimes – AADC non-justiciable

The AADC provides further guidance for the gaps found in legislation, namely how the digital space can be made safe for young people and a series of risk assessments in assessing the certainty of age to satisfy the DPIA. The crucial issue posed by the AADC is that a magnitude of discretion is given to digital platforms by providing recommendations rather than an enforceable legislative regime. This is seen where the AADC seeks to establish age assurances:

> "This code is not prescriptive about exactly what methods you should use to establish age or what level of certainty different methods provide. This is because this will vary depending on the specifics of the techniques you use. We want to allow enough flexibility for you to use measures that suit the specifics of your individual service and that can develop over time."[247]

The AADC lacks precise instruction, definition, and enforceability. The code should have the capacity to demand legal action (such as compensations of fines) if the platforms ignore the guidance. Otherwise, a lack of accountability and repercussions have taken away any incentive for the platforms to adhere to the AADC, particularly when their main objectives are data collection and profit. There is no reason for the AADC to promote 'flexibility'; providers cannot choose from a selection of enforceable AADC.

[245] Information Commission, 'Information Commissioner's Opinion: Data protection and privacy expectations for online advertising proposals,' (2021) 16

[246] Article 19 Data Protection Working Party WP 217 2014

[247] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 33.

The code was drafted in response to their recent national survey into the biggest data protection concerns, finding that children's privacy is second only to cybersecurity. Their results showed that one in five digital environment users are children (as opposed to adults), yet the digital space was not designed for them.[248] This report will demonstrate the ineffectiveness of the code at its core: the report is riddled with *recommendations*,[249][250] instead of legally enforceable regimes.

4.6 Recommendations

There are possible technical solutions that could promote children's digital rights by design. Elimination by removing commercial interest in tailored content would not immediately resolve the issues because the harm is instinct to technology as opposed to solely from the content shown. It is the responsibility of the platforms to mitigate harm by design before reaching the child. Aside from content, there are intrinsic problems with Big Tech data sets driving decision making. From this perspective, it is arguable that Instagram' explore' pages should not be present in children's social media accounts, as this would remove potentially harmful content and prevent the 'mindless' scrolling that these pages are specifically designed to stimulate. Similar features on other platforms include YouTube and TikTok autoplay feature designed by data profiling. The task then falls to regulation or design, mitigating the harm of the design of the platforms before they collect data to personalise content.

(a) Age assurance design

An alternative age assurance measure is the need for a parent or guardian to approve or deny the account if a child attempts to recreate a social media account. The parent is therefore aware that their child is using social media and enables them to monitor usage. Two links can be sent to the parent: one to confirm or deny the account and another to set the privacy settings. If this child later wishes to change these settings, instead of the AADC pop-up recommendation to seek guidance from an adult (which the child can swipe away), approval will need a PIN sent to the parent's email account or require facial recognition from an adult.[251] These are more substantial measures to ensure the child is not left to their own accord when using social media.

[248] Ibid.
[249] For example, ibid 34, 40, 43.
[250] For example: Age Appropriate Design Code 34, 40, 43
[251] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 38.

Instead of solely relying on providers to deter underage children from accessing the platforms, greater preventative action should be crafted to disengage the child. For example, once the child attempts to resubmit their age, they are met with a series of 'bite-size' information blocks that explain what harm may arise if they try to access the platform. Assuming the user is under thirteen (the DPA minimum age for consent and often social media platforms minimum age requirement), it can be gently explained that the platform is too old for them, like seeing a scary movie with too high an age rating. Children understand the concept of age-rated movies, so why not age-rated platforms? The platform then may redirect them to speak to a trusted guardian or teacher about having a social media account. This is unlikely to deter the child who may be persistent, especially if all their friends have an account. However, it does incorporate parental guidance in accessing a social media platform, rather than the child continuously attempting to create an account of their own accord.

AI and third-party verification services are viable solutions in establishing true age. Regarding the AI, the AADC states:

> "It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with your service. Similarly you could use this type of profiling to check that the way a user interacts with your service is consistent with their self-declared age."[252]

And for third-parties verification:

> "Such services typically work on an 'attribute' system where you request confirmation of a particular user attribute (in this case age or age range,) and the service provides you with a 'yes 'or 'no 'answer. This method reduces the amount of personal data you need to collect yourself and may allow you to take advantage of technological expertise and latest developments in the field. If you use a third party service you will need to carry out some due diligence checks to satisfy yourself that the level of certainty with which it confirms age is sufficient."[253]

[252] Ibid 34.
[253] Ibid.

Both solutions are convincing and could be highly effective in establishing user age when used together. However, the AADC falls short of actually achieving these outcomes. These are the two most technical and resource-consuming models (in terms of time and costs) and are unattractive from a service provider perspective, as consumer safety and protection are not known to be the heart of their ethos. This has the benefit of identifying users who are too young for the service, thereby deterring false declarations of age and ensuring that content is matched to the true age of the account. However, the use of a third-party verification service may bring fresh problems of additional profiling and data collection, which may require further regulation and therefore creates a circular issue. Moreover, there may be greater risks associated with inaccuracy and discrimination, which may further infringe the fundamental rights of a child.

To mitigate these concerns, the AADC could provide a vetted list of third parties, which provides a variation of companies that can suit the differing amount of data collected from different platforms. Additionally, instruction on how AI can determine age would be beneficial, alongside a set of instructions about how to implement it onto the platform

(b) DPAI

Platforms are not required to publish DPAIs; they are only encouraged to do so out of 'good practice', thereby impeding open access and accountability. DPIAs should be mandatory for *all* platforms that may *potentially* engage with young persons and collect their data. Such a policy would promote:

- better completion DPAIs;
- stronger child protection community in the digital space;
- increased transparency for people to access DPIAs and gain more information about the platforms they use (especially for newer platforms such as TikTok);
- accountability for platforms to take adequate steps to ensure safety.

It may also be beneficial to introduce a specific statutory requirement that the DPIA must be completed before processing to ensure that the outcomes are used in the platform's design before the launch. Additionally, we recommend that DPIAs be completed by all platforms currently operating. This casts a wide enough net to ensure that the infringing platforms are already processing data is compliant.

DPIA to consult children and parents should be mandatory for the assessment. Conducting Child Impact Assessments and making children visible in technology policy development. Consulting with the target audience as to whether they comprehend language used in service, privacy information, and pop-ups can provide valuable insight into the true workability and effectiveness of the safeguard measures. Online safety dually necessitates the child's behaviours and the influence of parents or guardians. A collaborative approach is valuable because providers can design their platform according to recommendations from parents, and parents are also encouraged to take a more hands-on approach to their child's digital use. Counsel from parents can provide credibility to the platform, which can be the foundation of a huge marketing push that could drive traffic.

Finally, DPIAs must be carried out if there is a high risk to the rights and freedoms of natural persons.[254][255] There is no definition of specifically what the risk may constitute, nor of the harm that may arise because of the risk. Despite the absence in definition, 'harm' is used informally on The Information Commissioner's website page to further guide controllers.[256] Guidance and effective compliance in general would surely benefit from a statutory definition of harm. Therefore, it may be helpful for the ICO to create a non-exhaustive list for potentially harmful content, such as violence, eating disorders, racism, and gambling. The list has the potential to be very expansive and instructive. If a platform has the *potential* (as a low threshold) to show young people content that falls under this list, they must then complete a DPIA.

[254] *GDPR* (n 55) Recital 75.
[255] Recital 75
[256] The Information Commissioner, 'Guide to Data Protection,' available at < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/>

(c) Other technical measures

Child protections by design could include 'opt-out' of essential cookies, which would have boundless implications for privacy. The platform would collect and process fewer data about the user, meaning that the likelihood of presenting sensitive content based on their preferences is less. Instead, the platform would show more 'generic' and age-appropriate content. If a child decides to opt-in, an alert could be sent to the guardian email account, as previously mentioned, which would then require their approval. If the account is not linked to a guardian, adequate 'bite-sized' explanations of the consequences of changing data collections should appear. Unlike the example provided in the AADC, the pop-up should contain a series of explanatory images accompanied by highlighted keywords and shorter sentences. The child must individually click through before consenting. For younger users, real-world analogies may be helpful. For example, returning to the age-rated movie example, changing preferences may be accidentally harmful, confusing, or 'scary' content, like if they glimpsed a movie meant for adults.

There should be a clear 'unsubscribe' feature for certain types of content, which means similar content will never be shown on the newsfeed again. It should be as easy as it is to unsubscribe from emails. For example, if a young child is shown gun crime and finds it distressing, a button should allow them to select: 'Don't show me this again. 'All similar content would then be wiped from the newsfeed. The child needs to be made aware that this is an option to implement. This can be signalled as they sign up to the platform, which typically includes a walkthrough tour. Alternatively, when a child clicks on harmful content, a reminder can pop-up suggesting that they can unsubscribe at any time.

Young children need to be informed of the data profile built on their preferences and the consequences of engaging with this type of content. When interacting with inappropriate content, a series of notifications can arise:

1. The first banner arises, explaining that you will see similar content on the newsfeed if you click on this.

2. The child is then presented with a choice: *Do you want to see more of this content?*

3. 'Yes,' or 'No' will be the options.

4. For particularly harmful content, nudging techniques can be used to make the 'No' selection more attractive, such as using a bold font or appeasing colours (i.e., green for No and red for Yes).

5. If the child chooses 'Yes', a secondary banner arises, explaining that the platform collects their interests to create a data profile. If they click Yes, the platform will record it as an interest of the user and create a data profile. For example, if *you click yes, we will record this as something you are interested in to create a digital profile to show you similar stuff. Are you interested?*

This adequately informs the child, deters discrimination in inaccurate data profiles, and hopefully deters the risk of children snooping to find inappropriate content.

In response to the AADC, YouTube recently changed the settings for autoplay to turn it off by default for users aged thirteen to seventeen. This should be a design feature for all platforms, especially TikTok and Instagram, that use personal data to automatically extend engagement instead of requiring children to make an active choice about whether they want to spend their time in this way (known as data-driven auto play features).

Box 17: Recommendation for removing endless scroll

Platforms can enforce a 'respite' period to prevent continuous usage. For example, if a child has been using a platform for over an hour or two, the platform can force them to take a break by remaining frozen or not refreshing for the allotted time. Every hour, there may be a mandatory respite. Or, for every two hours, there is a twenty-minute respite. A banner will arise that informs the child what is happening and why in a friendly manner: *Yikes! We noticed you had been online for two hours. We will now take a break and will refresh in twenty minutes. Why don't you use this time to do something else?* The notice can be made humorous, which is likely to engage young adults. Most notably is Netflix's pop-up of *Are you still watching?* After a user has been streaming for serval hours at a time, which has circled the digital environment in various memes.

Similarly, Instagram's new 'Take a Break' feature and 'Daily limit' are pop-ups to encourage users to stop using the app after a certain amount of time and break the cycle of endless scrolling. 'Take a Break' is automatically implemented, but the Daily limit must be set-up by users according to their preference on the amount of time they wish to spend on the app per day. Although these additions are certainly a step in the right direction, their effectiveness is questionable given that a user can easily swipe away the reminders and continue scrolling. It is particularly unclear how effective they will be for children. A time-conscious adult, who is exposed to the public perception that society spends too much time scrolling, is likely to engage with these features. However, children require a more interventionist and paternalistic approach. A more effective model for children would be to disable the app for a short amount of time for the 'break' and physically force the child to stop scrolling. This should help break the endless cycle of scrolling and encourage the child to engage in other tasks.

5 Gaming

5.1 Background

Digital gaming space and children's interaction pose several threats to children’s rights as envisaged in the UNCRC, including the GC No.25. In this report, firstly, there is a discussion of the various forms of online harm that threaten the children in the online gaming space, thereby providing context for succeeding sections. Then, different issues are discussed, such as loot boxes, far-right extremism, self-harm, bullying. Most importantly, the design features used for perpetrating such online harm to children are also explained. After that, a discussion on the key child rights/principles from the UNCRC and GC No. 25 directly affected in relation to online gaming is provided. Herein, some of the primary principles (‘best interests’ principle, non-discrimination principle, etc.) along with some others that are directly relevant to the online gaming space (right to leisure, culture and play, freedom of expression, etc.) are discussed highlighting the impact of the online harms of the digital. In the succeeding sections, the current legal framework and the gaps thereby are discussed, highlighting the current laws and policies of the online safety regime, such as the Gambling Act, Draft Online Safety Bill, the Online Harms White Paper, etc., and the gaps that exist therein, which make the legal framework relatively crude for the sophisticated harms endangering children in the gaming space. Finally, the report attempts to capture the fragmented suggestions that have been extended by various resources and analyses them to evaluate their contribution to the development of the regulatory framework of the digital gaming space.

5.2 Digital participation and potential harm

(a) Gambling

One of the key concerns arising from online gaming activities is gambling-like behaviour. The connection between online video games and gambling is a growing concern. It affects children in unwanted ways by making them develop addictive behaviours without being physically involved in conventional gambling activities.[257] Online gaming includes features like in-game purchases. Games that are Free to Play (**F2P**) commonly use these purchases to monetize an otherwise free game.[258] Many online games include a special in-game feature called a loot box. Loot boxes are in-game purchases that players buy using real money or in-game currency (which also exhaust at some point and might have to be bought using real currency).[259] These boxes contain a random selection of items revealed only upon opening the box. The contents usually contain game-specific prizes such as advanced tools, costumes, hairstyles, accessories, etc. They can also contain other items that improve the player's odds by providing energy boosters, weapons, etc.[260] Specific examples of loot boxes games are Clash of Clans, FIFIA, NBA, Fortnite, etc.[261]

Box 18: Loot boxes and digital harm

Loot boxes are a major concern in relation to child rights in the digital environment because of their gambling-like nature.[262] There is uncertainty and anticipation in relation to these online prizes that are bought with real money. This aspect of uncertainty with other 'nudge techniques'[263] makes it attractive and addictive for children. The excitement to open the boxes or the excitement of the revelation of the contents of the boxes, the disappointment (sometimes) with the contents of the boxes and hence, the powerful urge to purchase more boxes, and so on, are all characteristic of gambling behaviour and these loot boxes encourage such behaviour among children.

[257] Children's Commissioner, *Gaming the System* (October 2019) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2019/10/CCO-Gaming-the-System-2019.pdf>.
[258] Ibid.
[259] Rob Davies, 'Video Game Loot Boxes Linked to Problem Gambling, Study Shows', *The Guardian* (online, 1 April 2021) <https://www.theguardian.com/society/2021/apr/02/video-game-loot-boxes-problem-gambling-betting-children>; 'Loot Boxes Linked To Problem Gambling In New Research', *BBC* (online, 2 April 2021) <https://www.bbc.co.uk/news/technology-56614281>.
[260] Children's Commissioner, 'Gaming the System' (n 257).
[261] Ibid 5–7.
[262] Annette Cerulli-Harms et al, *Loot Boxes in Online Games and Their Effect on Consumers, in Particular Young Consumers* (No PE 652.727, July 2020) 56.
[263] Children's Commissioner, *Gambling Act Review* (2020) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2020/11/cco-gambling-act-review.pdf>.

Surveys show that in-game purchases are the most common spending, indicating the success of mechanisms such as loot boxes in terms of encouraging addictive expenditure for instant gratification. Loot boxes are instantly accessible and make it convenient for children to continue spending without any wait time, complex processes, or parental supervision (and even knowledge, in some cases).[264] Moreover, another characteristic feature associated with gambling is the behaviour of 'chasing losses,'[265] i.e., recognising the addiction and the powerful sense of guilt in the player, despite which they cannot stop. Such a sense is also felt by the children who participate and spend significant amounts of real money on loot boxes, who also feel the burden of wasteful expenditure.[266]

Another aspect of the gaming world that promotes gambling-like behaviour is the usage of skins in video games. While using skins as a form of currency to trade is currently considered gambling under the Gambling Act 2005, the skins themselves remain unregulated.[267] The reason is the same as loot boxes, i.e., they do not have a monetary prize. Therefore, skins can still be easily purchased, obtained by opening loot boxes or won in a game. This demonstrates ignorance or limited understanding of the real effects of these items, ultimately resulting in allowing children to become subject to gambling-like features and behaviour during online gameplay.

In conclusion, the accessibility of the loot box form of in-game purchases in online games is problematic. By their nudge techniques and instantly gratifying features, Loot boxes encourage addictive gambling-like behaviour and wasteful expenditure while also burdening children with a sense of guilt and feeling trapped.

[264] Ibid 1–2.
[265] Children's Commissioner, 'Gaming the System' (n 257) 27.
[266] Ibid 23.
[267] Select Committee on the Social and Economic Impact of the Gambling Industry, *Gambling Harm— Time for Action* (2 July 2020) 110, paras 423, 424 <ttps://committees.parliament.uk/publications/1700/documents/16622/default/>.

(b) Priming Mechanism

The priming mechanism is important from the perspective of the effect of online games on children's behaviour and hence, needs a much more granular understanding of the impact of gaming space. With video games, studies have identified that "specific concepts" depicted in the games affect the child's behaviour by priming such concepts.[268] In terms of models, there are General Learning Model (GLM) and General Aggression Model (GAM). [269] The GLM is the model that is mostly used to explain the change in the player's (in this case, a child) behaviour.[270] Under this model, the specific concepts depicted in the game raise reactions from the children, enabling the priming of that concept, i.e., impacting their behaviour.[271] While this impact could be temporary, longer durations of exposure to such games and the concepts thereof would have lasting impacts on the child's behaviour through "reinforcement".[272] Hence, priming has become an important aspect of the digital gaming space, especially gambling-like features and violent concepts in games. Loot boxes and skins become more problematic because of the priming mechanism, as the concept of gambling gets primed to affect the children's behaviour. In relation to violence, it is understood that GLM is an extension of another model called GAM, wherein the concepts related to aggression like weapons, violent concepts, etc., are reinforced in the children's behaviour through priming. Hence, priming mechanisms explain the importance and urgency of regulating extreme violent content or gambling-like features in the games. The rewards that children obtain from participating in features such as loot boxes, the underlying concept, i.e., gambling, gets reinforced in the children's behaviour. Such behavioural changes are much more problematic, but because of the gaps in the legal framework in relation to loot boxes and/or priming mechanism relating to the reward loop mechanism *per se*, it is difficult to regulate them.

---

[268] David Zendle, Paul Cairns and Daniel Kudenko, 'No Priming in Video Games' (2018) 78 *Computers in Human Behavior* 113 <https://linkinghub.elsevier.com/retrieve/pii/S0747563217305472>.

[269] Ibid.

[270] Ibid.

[271] Ibid.

[272] Katherine E Buckley and Craig A Anderson, 'A Theoretical Model of the Effects and Consequences of Playing Video Games' in *Playing Video Games: Motives, Responses, and Consequences* (Lawrence Erlbaum Associates Publishers, 2006) 363.

However, it is noteworthy that recent experiments have provided the concept of negative priming, as the experiments have shown that upon exposure to specific concepts in the games, the players in the sample survey have shown that they are rather slow in reflecting those concepts in their behaviour.[273] The concept of negative priming has made the impact of priming's reinforcement aspect inconclusive. However, this is an avenue for further research, maybe sponsored by the government to understand the impact of the games through priming mechanism as negative priming can be used in furthering/preventing furtherance of gambling-like behaviour or aggressive behaviour.

(c) Extremism & Bullying

This section aims to highlight the growing concerns of bullying and extremist (especially far-right extremist) content that children are exposed to via online gaming. While bullying and extremism are very different and separate issues, they both share the commonality of being made accessible to children via chat mechanisms associated with online games. Many chat platforms have come up to respond to the growing online gaming community to provide a space to connect. Some examples of such platforms include Discord, Overtone, etc. Gamers can use other platforms to conduct live streaming as well. These spaces allow profuse interaction between the gaming community, including children. While these platforms help children develop meaningful friendships, they also raise serious concerns over bullying and extremist content.

[273] Zendle, Cairns and Kudenko (n 268) 8.

The concerns over the spread of extremism via these spaces, although significant, remain anecdotal. There are several instances where children and their parents/caretakers have raised concerns about being targeted by extremist groups.[274] Official exploration of such occurrences in the gaming industry is notoriously low. Far-right extremist groups use chat systems such as Discord to influence children and groom them towards radicalisation.[275] Upon research, it has also been found that there are certain right extremist groups on the chatting platforms that specifically intend to target UK children.[276] The extremist contents also contain anti-Semitic content. For instance, a 12-year old child was targeted by extremists who flooded the group chat with neo-Nazi propaganda.[277] The extremists entered the group chat when one of them was allowed entry by one of the children in the group itself.[278] A tactic used by extremists is to interact in a friendly manner and talk about game-related aspects with the children, thus making themselves reliable and making the kids feel comfortable.[279] After that when they are let into private groups chats on chat platforms such as Discord, etc., they gradually start introducing extremist ideas, visuals and propaganda, thereby gradually influencing the children's opinions and actions.

Further, another aspect of this issue that makes it a dangerous concern is the language used by the extremists to interact with the children. Often, suppose the games involve violent content. In that case, the violent/extremist language can be easily masked by the game's specific terminology, which develops into a code language that is difficult to identify and address.[280] Again, the age group, i.e., children, are vulnerable groups, and not addressing these loopholes or gaps in the gaming industry in terms of, among other things, design, puts children at significant risk.

---

[274] Jacob Davey, *Gamers Who Hate: An Introduction to ISD's Gaming and Extremism Series* (ISD, 2021) <https://www.isdglobal.org/wp-content/uploads/2021/09/20210910-gaming-reportintro.pdf>.
[275] Ed Nightingale, 'Young People Reportedly at Risk of Far Right Extremism through Online Gaming Channels', *Eurogamer* (27 April 2022) <https://www.eurogamer.net/young-people-reportedly-at-risk-of-far-right-extremism-through-online-gaming-channels>.
[276] Ibid.
[277] Misha Valencia, 'A Hate Group Targeted My Kid Online - The New York Times', *New York Times* (online, 8 September 2021) <https://www.nytimes.com/2021/09/08/parenting/online-hate-groups-kids.html>.
[278] Ibid.
[279] Linda Schlegel, *Extremists' Use of Gaming (Adjacent) Platforms: Insights Regarding Primary and Secondary Prevention Measures* (European Commission, Radicalisation Awareness Network, 2021) <https://ec.europa.eu/home-affairs/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf>.
[280] Ibid.

The gaming community's risk of bullying will also be discussed in this section because the same feature is often used for this purpose. Whether the communication between the minor gamers happens through chatting platforms exclusively dedicated to the gaming community or in-game chat features, bullying through these spaces is a huge concern. As can be seen from many anecdotes, the issue of bullying in online games is also related to the issue of loot boxes and is one of the reasons for the increased use of loot boxes.[281] Children have admitted that the 'privacy of headsets' and the online chatting platforms allow their peers to say things they would otherwise hesitate to do in person, which progressively leads to teasing and bullying.[282] Bullying happens for various reasons, one of which is not having advanced skills or new skins, which often requires the expenditure of money (as seen in loot boxes).[283] Bullying, like in reality, in virtual spaces can also implicitly result from the social status of the children, which is often determined by the ability to afford new skins/avatars/weapons, etc. Children sticking to the 'default skins' are bullied and feel embarrassed about their perceived 'poor' situation.[284] Bullying in the online gaming spaces has also been admitted by children, by hostile behaviour such as 'attempt to destroy the progress of a peer in the game', etc.[285] Although anecdotal evidence shows that children who are subjected to bullying often prevent engagement with the perpetrator by 'muting them' or 'blocking them' or 'reporting them',[286] it cannot be a reason to leave such spaces and such actions (which are otherwise strictly regulated in real life), to escape regulation just because they are happening in the virtual sphere. One of the perceived incentives of the people involved in this interaction as a bully is that their questionable actions are not consequential, so there is a requirement to address this concern. The negative impacts of bullying are well-established, and hence, steps must be taken to regulate and prevent the same in every aspect of a child's life, including the time spent in the virtual world. Gaming is an extension of the offline lives of the children, and hence, the regulation/supervision applicable should be the same.[287]

[281] Children's Commissioner, 'Gaming the System' (n 257) 2.
[282] Ibid.
[283] Ibid.
[284] Ibid.
[285] Ibid.
[286] Ibid.
[287] Ibid 3.

(d) Self-Harm

The CRC defines a child as below 18 years of age (except in cases where the national law provides for an earlier majority age).[288] This age group includes adolescents as well. In the online gaming world, although not exclusively, this age group is also targeted for games that encourage self-harm and suicidal actions. One such game, which became somewhat of a phenomenon, was the 'Blue Whale challenge'.[289] The number of children taking their own lives to fulfil the challenge was shocking, and although the challenge started in Russia, it soon travelled overseas, including to the UK. Upon research, it was also found that there were several online chat groups wherein adolescent children talked about depression, self-harm, suicide, etc., without any supervision whatsoever.[290] And it was in one such chat system where the Blue Whale game was spreading.[291] The game's administrators also found that it would reach out to the underage teenagers on different fora such as WhatsApp, Facebook, etc., and encourage them to take up the challenge.[292] The difficulty in banning such a game was that it was not an application that had to be downloaded onto a device to be accessed but was accessible when the administrators would contact the prospective users.[293] Hence, preventive response (such as monitoring the browsing time, the browsing history through parental control design features[294] or, as psychiatrist Harish Shetty calls, "gadget hygiene")[295] becomes more important. While concerns surrounding the privacy of children might come into the picture when children are getting monitored by their parents, it must be understood that in the absence of such monitoring, the data and information of these children land up in the hands of the gaming administrators, who have an incentive to misuse such information. Further, more sophisticated mechanisms would require fathoming several possible self-harm encouraging techniques adopted by such online games and addressing them through comprehensive legislation.

---

[288] *CRC* (n 1) art 1.

[289] Ant Adeane, 'Blue Whale: What Is the Truth behind an Online "Suicide Challenge"?', *BBC News* (online, 13 January 2019) <https://www.bbc.com/news/blogs-trending-46505722>.

[290] Ibid.

[291] 'Blue Whale Game: Here's Why Experts Think It Is Not Possible to Ban the Blue Whale Challenge - The Economic Times' <https://economictimes.indiatimes.com/magazines/panache/heres-why-experts-think-it-is-not-possible-to-ban-the-blue-whale-challenge/articleshow/59941418.cms?from=mdr>.

[292] Ibid.

[293] Ibid.

[294] Ibid.

[295] 'Psychiatrist Dr. Harish Shetty on How to Prevent Suicidal Tendency in Kids', *Mid-day* (4 August 2017) <https://www.mid-day.com/lifestyle/health-and-fitness/article/emotional-stress-depression-psychiatrist-dr-harish-shetty-blue-whale-game--18480180>.

5.3 Child rights opportunities and impacts

(a) Non-discrimination

One of the General Principles as per the GC No. 25 is the principle of Non-Discrimination.[296] According to the GC, the State parties must ensure that there is no "digital exclusion" of children, among other things, through the use of "hateful communications" or "unfair treatment" in the digital space. In relation to the gaming space, this is relevant with regard to cyberbullying, which can happen on the basis of race, gender, etc. and can cause digital exclusion. This can also occur in cases of loot boxes, wherein exclusion or bullying might happen based on "socio-economic background" (lack of advanced levels of weapons or skins or abilities in a game can cause abuse/bullying and consequent embarrassment based on socio-economic background, which can cause "discourage participation" in the digital space).[297]

Furthermore, it is also important to recognise that digital gaming spaces provide immense socialising opportunities for children with disability.[298] However, if during communication with their peers in the gaming space, there is a sense of hatred or non-inclusivity of disability in general or if children with a disability feel like they have should hide their disability to be not bullied or to be included in the socialising sphere. This principle of non-discrimination is being compromised. The other, more generic form of discrimination in the gaming sphere is the general lack of representation of female protagonists (or the predominant presence of white males as the protagonists)[299] in the games and female characters rather than being used in a sexualised manner.[300] This tends to impress problematic conceptions of females in the minds of both male children and female children. It is important to recognise that digital gaming space, which is one of the most used spaces by children of this age, can bring transformative discourse in tackling gender stereotypes, racism, etc.[301] Hence, State parties must consider these aspects of the digital gaming space and address/redress the issues to uphold the principle of non-discrimination in this space.

[296] *General Comment No. 25* (n 2) 2.
[297] Daniel Kardefelt-Winther, *The Online Gaming Industry and Child Rights* (Innocenti Discussion Paper, September 2019) 10 <https://www.unicef-irc.org/article/1926-the-online-gaming-industry-and-child-rights.html>.
[298] Ibid 17.
[299] Ibid.
[300] Ibid 16.
[301] Ibid 17.

(b) Best interests of the child

The 'best interests' of the child should be one of the core guiding principles underlying any legal regime/instrument intended for the protection of the rights of the child. The GC explicitly recognises that the digital environment was not made exclusively for children. Yet, the space is extensively used by children and hence, safeguarding the 'best interests' in this forum becomes even more crucial.[302] It explicitly calls upon States to have the best interests of the child as the highest priority while considering regulations, design, management, etc., relating to the digital environment.[303] Crucially, the GC also provides that due regard should be given to, *among other things*, the right of children 'to be protected from harm', transparency in the assessment of the best interests, and the criteria used for it.[304]

'Best interests' are a vital consideration in relation to the gaming industry because of the extensive engagement of children with the industry and the primary profit motive of the corporations involved in providing the gaming services. Like any other industry, the online gaming industry is driven by the profit motive, and hence, the construction of the digital spaces within these games is mainly to serve that purpose. Most often than not, these profit-centric interests are not in alignment with the best interests of the child; rather are achieved at the cost of the same. Hence, the 'best interest' considerations become a vital focal point in the field of online gaming. The design of these games often compromises on this principle of the CRC, and States have a heightened duty to regulate this industry with apposite and updated laws/regulations to ensure that every entity involved in the production/distribution/management of these spaces has the best interests of the child as their primary consideration.

[302] *General Comment No. 25* (n 2) 2.
[303] Ibid 3.
[304] Ibid.

(c) Right to life, survival and development

In relation to the gaming industry, the right to development is another important right that is potentially affected. The GC recognises the role played by the digital environment in the development of children.[305] Online games allow children to react to a range of simulated situations, which otherwise might be impractical or impossible for children to face, thereby allowing the development of skills such as intelligence and physical agility.[306] In particular, the GC recognises that the digital environment can help children develop skills that can be especially useful during a crisis.[307] However, certain online harms severely affect the development of children in an adverse manner. Such online harms include extremist ideas and bullying. They affect children's opinions and mental health, respectively. The former does not allow children to view the world in a grounded, neutral perspective and organically and independently develop an understanding and preference with respect to ideologies. The second online harm of bullying significantly affects the mental well-being of children as they might feel isolated and embarrassed, and these feelings may also be compounded by the fact that the bullying is occurring in a virtual world. Furthermore, bullying in the digital environment may be more severe than conventional bullying in the schoolyard, as there is less hesitancy and restraining social considerations associated with carrying out bullying actions online than physical presence. A child's right to life and survival can be endangered by challenges like the Blue Whale, which encourages children to take their own lives.

[305] Ibid.
[306] Ibid.
[307] Ibid [14].

(d) Respect for the views of the child

The GC No. 25 provides another cardinal principle of child rights, i.e., the principle of "respect for the child's views". The GC recognises that the digital space has opened new avenues for children's participation in many discussions, especially related to them. In the gaming sphere, this mainly becomes relevant, which the GC emphasises, i.e., when laws and policies are formulated in relation to digital space (including gaming space). The GC captures the need to consider children's views while formulating laws and policies on digital space.[308] However, it is noted that in many instances, the inclusion of children in such processes is limited to the form of research subjects. For instance, the anecdotes shared by children regarding the impact of loot boxes in the games on themselves in the report of the Children's Commissioner is an apt illustration of children being involved as research subjects. While this is an important way of including children, it should not be the only way. Children should be actively included in consultation processes of legislations that concern their digital environment, especially relating to online gaming. However, it is not the case, as can be seen from one instance, which is the consultation process for Online Harms White Paper. As per the demographic information provided, children (below 18 years old) constitute only 5% of the responses received (the largest proportion belonging to ages 45-54).[309] This is also necessary to ensure the protection of rights to privacy and freedom of expression.

(e) Right to leisure, play, and culture

Right to leisure, play, and culture is directly related to the digital gaming space. However, it is important to notice that the right contains both "leisure" and "play". This implies that if digital gaming space, meant to be an entertaining, relaxing, and joyful experience for children, becomes stressful and disturbing, then the right to leisure is hampered. Hence, the right to play must be balanced with the right to play. This can be done by addressing the adverse issues found in the digital gaming space, such as loot boxes (resulting in economic exploitation) and cyber-bullying (resulting in psychological distress), etc. The GC provides that it is the shared responsibility of States, service providers, parents, etc., to ensure that the digital spaces that impact a child's leisure time should contribute to their recreation. The right to culture is also a crucial aspect of digital gaming space because interaction with peers occurs across countries and regions, allowing children exposure to cultural diversity.

"Play is one of how children develop the ability to express themselves early on. Therefore, it is vital that they have opportunities to play and participate in recreational activities, cultural life, and the arts."[310]

[308] *General Comment No. 25* (n 192) 3 [17].
[309] {Citation}
[310] Child Rights International Network (n 23) 13.

However, interactions that result in digital exclusion through bullying based on racism or sexism might have highly adverse impacts as well, which also relates to hampering their freedom of expression. Similarly, extremist content shared on such chatting platforms can affect children's viewpoints imbalanced, resulting in ethnocentrism. These issues related to gaming spaces must be addressed to ensure that this right of culture is preserved.

(f) Protection from economic, sexual and other forms of exploitation

The GC provides that [311] children can be called economic actors in a digital environment by' creating and sharing content'. However, such a situation can also result in the exploitation of the children, as also recognised by the GC. This implies that the understanding of child labour must be more nuanced with the digital space so that possible exploitations of children are captured and presented in these spaces.

Children act as game content creators and earn their share of profits. For example, in the case of Roblox, children are trained to create gaming content through child-friendly versions of tools using which they create the gaming content, which Roblox then uses to share with other children.[312] Upon the success of such gaming content, the child creator(s) get the requisite share of profit. Elements of employment clearly exist in these situations. While prima facie, it might appear that such a situation does not involve child labour because it involves creating gaming content that a child does out of the free will, there is a requirement for a more nuanced understanding of the situation.

There is child labour involved because Roblox gains profits from its gaming content, which children create. Further, the advertising of the games is also done by children as Roblox invites children to play the games, which is then popularised among the children's groups.[313] For instance, Anna, a child creator from Roblox, admits that "she saw herself as a partner in the venture where her skills proved invaluable".[314] The income so received by some of the child creators was not under a legal contract, for which a guardian must be involved (because the children are not eligible to enter into contractual agreements) but were mere informal settings and depended on the whims and fancies of the owners. However, the child-creators were converted into "independent contractors with fixed salaries" when the situation changed.[315]

---

[311] *General Comment No. 25* (n 2) [112].
[312] Bree Royce, 'Roblox's Shameless Exploitation of Child Labor Is Why We Can't Have Nice Things', *Massively Overpowered* (20 August 2021) <https://massivelyop.com/2021/08/20/roblox-is-why-we-cant-have-nice-things/>.
[313] Ibid.
[314] Simon Parkin, 'The Trouble with Roblox, the Video Game Empire Built on Child Labour', *The Gu* (online, 9 January 2022) <https://www.theguardian.com/games/2022/jan/09/the-trouble-with-roblox-the-video-game-empire-built-on-child-labour>.
[315] Ibid.

Additionally, instances of blatant exploitation are rampant, considering the creators are of a young age group dealing with professional engagements with no training on interpersonal skills in such an environment. Further, Anna's story shows how possible intellectual property issues (as the game created by the child -the creator is sold without any remuneration to the child who quits the venture) can crop up, leading to more intense exploitation. The absence of a Human Resources team is another concern with Roblox. While human resources are being used for gaining profits, many issues like what an employee faces in a normal work setting are also faced by these child-creators. Still, there is no recourse available to address these issues. For instance, Jaden's story shows that while children are acting like usual employees working overtime and having consequent mental/physical health issues, there is no recourse available to address such exploitation either in terms of increased remuneration (overtime salary) or in terms of compensation.[316] Further, another shortcoming that these scenarios deal with can be seen in Rachel's story. While she was effectively performing an employee's/service-supplier's job without any involvement of her guardians/parents to file a complaint against the venture she was asked to accompany her parent.[317]

In short, our lack of nuanced understanding of child labour, with new scenarios cropping up in the digital space, has made the exploitation of children by video game companies like Roblox possible. Because while such companies involve children in literally every action that an employment or service-supplier under contract provides, there is no law to protect the conditions under which such dealings happen, thus resulting in the exploitation of children (mental health issues, no remuneration profit-sharing, possible intellectual property rights violations, sexual harassment at 'workplace' issues) who are left with no redressal mechanism, whatsoever. Hence, recognising GC of children's interaction with the digital environment as a content-creator and the consequent exploitation thereof is welcomed.

5.4 General measures of implementation by the United Kingdom

(a) Legislation

The relevant UK legislation dealing with the issue of children's rights in a digital environment is notoriously recent. For some issues related to gaming, they are yet to be made. Therefore, this section will focus on existing or prospective laws that deal with the issues discussed in the earlier sections.

[316] Ibid.
[317] Ibid.

Gambling Act 2005

The Gambling Act 2005 (Gambling Act) provides the regulatory framework for gambling activities in the UK. The regulator in this industry is the Gambling Commission. The Gambling Act intends to regulate gambling activities in the UK. For the purposes of this report's theme of gaming, the relevant provisions of the Gambling Act in relation to the link shared between gambling and gaming are sections 3 and 6. These two sections provide definitions of 'gambling' and 'gaming'. According to the illustrative (and exhaustive) definition in section 3, 'gambling' means 'gaming',[318] 'betting',[319] and 'participating in a lottery'.[320] All these terms are defined in the legislation. For our purposes, 'gaming', defined in section 6 of the legislation, is important. Section 6 provides that 'gaming' refers to 'playing a game of chance for a prize'.[321] The provision also defines the terms 'game of chance' and 'prize'. A 'prize' is defined as the 'money or money's worth'.[322] These terms are crucial as they provide the context in which the gaps in the current law, i.e., the next section, will be examined.

Age Appropriate Design Code

The new Age-Appropriate Design Code (**AADC**) deals with gaming services head-on by including the same in the ambit of 'Information Society Services' (**ISS**).[323] The application of the AADC does not depend on whether remuneration comes from the end-user or not, which means that games that are F2P but obtain their funding through advertisements fall within the scope of ISS.[324] According to the AADC, certain standards must be followed by ISS providers. Some of the standards that are especially relevant for this report are 'default settings', 'parental controls', and 'nudge techniques'.[325] These standards are highly important in regulating the gaming industry in light of their employment of loot boxes, advertisements targeting children, and provision of chat services (or chat services that are separately created but exclusively used for the gamers' community). Indeed, the issues discussed earlier in this report associated with these features of online games can be resolved through the AADC standards.

---

[318] *Gambling Act 2005* s 6.
[319] Ibid s 9.
[320] Ibid s 15.
[321] Ibid s 6(1).
[322] Ibid s 6(5)(a).
[323] Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' (n 58) 15–16.
[324] Ibid.
[325] Ibid 7–8.

(b) Comprehensive policy and strategy

Online Safety Draft Bill and White Paper

The Draft Online Safety Bill (the Bill) focuses on certain types of "internet services", which are defined as "regulated services" in the Bill.[326] The Bill's main objective is to specify the services and the providers of such services that the OFCOM (the regulator body introduced under the Bill) has the duty to regulate. The definition of "regulated services" is crucial because that will determine whether online gaming services fall under the ambit of the Bill or not. It is noteworthy that "regulated services" refer to two types of services: "user-to-user services" (U2U) and "search services". This is because the possibility of inclusion of gaming services will primarily be under the "user-to-user services". According to the Bill, U2U services refer to services that enable user-generated content that other users can access. This would include direct messages as well as they are user-generated content accessed by other users.[327] This aspect allows us to argue that the gaming platforms with extensive customised features for intra-gaming conversations and chatting systems or chatting platforms exclusively associated with online games (either by practice or by design) fall under this ambit.

Chapter 2 of the Bill provides the detailed regime for regulated U2U services. While the Bill provides for a general "duty(ies) of care" for the U2U services, it also specifically provides additional duties for user-generated content accessible to children. Hence, the service providers in the digital gaming space will be obligated to observe these additional duties of care. The duties as provided for in Clause 5(4) of the Bill include the duty to perform "children's risk assessment", the duty to ensure online safety for children, and the duty of "reporting and redress" for harmful content. A detailed guideline for risk assessment has been provided in clauses 7(3) and (4), which provides for general risk assessment, risk assessment when the service-provider undertakes a change in design or operation, reporting to Ofcom in case any "non-designated content" harmful to children is detected, etc. Clause 7(9) provides for requisite definitions of the phrases used for risk assessment purposes, including the term itself. It also provides the headings of information that are to be assessed through such risk assessment process, such as the age groups of the user-base, level of risk from "primary priority content", "priority content", and "non-designated content", etc.

[326] *Draft Online Safety Bill* (n 149) 3.
[327] *Draft Online Safety Bill* (n 149) Explanatory Notes .

Further, clause 10 of Chapter 2 provides the detailed duties that must be fulfilled to fulfil the general duty to ensure online safety for children consists of man. Such duties include the duty to either prevent exposure to harmful content or protect children belonging to the age group at risk of being exposed to harmful content if prevention is not possible. Hence, the Bill provides detailed obligations, i.e., duties of care that the services providers of regulated U2U services must fulfil. The regulation of these providers is to be done by Ofcom, as designated by the Bill.

To understand Bill's scope, it is also important to understand the ambit of "harmful content" in children's online safety. Clause 45 of the Bill outlines a detailed provision enlisting the meaning of "content that is harmful to children". At the outset, it provides general conditions for content to fall under this category. Then, it provides more specific characteristics that this content should possess to be categorised as "content that is harmful to children". For instance, in clause 45(3), it is specified that if according to the provider ("on reasonable grounds"), there is a "material risk" that the content will cause a "significant adverse physical or psychological impact" on a child, then that will fall under this category of harmful content. This is particularly relevant for content that is related to cyber-bullying and abuse. However, a problem might arise from the aspect that the judgement of such content is left to the service provider, and there are many subjective elements such as "reasonable grounds", "significant adverse harm", "material risk", and "child of ordinary sensibilities", etc. At the same time, the subsequent sub-clauses provide for the criteria that the service provider should consider while assessing the impact of a particular content [for example, Clause 45(6)], which only makes it less subjective but not objective.

For content relating to extremism, especially terrorism, Chapter 4 of Part 4 of the Bill is relevant. It provides for Ofcom's power to issue a "use of technology notice"[328] when, according to Ofcom, the provider is not complying with the requirements of substantive obligations under the Bill. The notice is an indication of the fact that the provider is required to "use accredited technology" to detect the "public" terrorism-related content and take it down (in the case of U2U services).[329] While clauses 63 and 64 provide for this direct power to Ofcom to tackle terrorism-related content, the Bill provides a much more comprehensive regime for dealing with terrorism-related content. For example, the phrase "offences related to terrorism" is provided with an explanation in Schedule 2 of the Bill. Still, a question is whether far-right extremism will fall under these offences because prima facie, it does not seem to be the case.

[328] Ibid clause 63.
[329] *Ibid clause 64(4)(a).*

Extremism as online harm is well-recognised in the Online Harms White Paper. However, extremism via gaming platforms and its associated chat spaces with the potential to target children has not yet gained the attention it deserves. The White Paper provides for a 'new statutory duty of care,[330] for the companies to be more mindful of the safety of their users and keep a check on the possible online harm that can be inflicted on them via the use of the concerned platforms.[331] However, it does not consider the major issues associated with the online gaming industry, including far-right extremist and terrorist ideologies. It refers to these issues only concerning the limited context of social media.[332]

The White Paper also provides a table listing the online harms covered under its ambit and divides these harms as per the extent of clarity of the definition. For example, it puts 'cyber-bullying and trolling' and 'extremist content and activity' under the category of 'Harms with a less clear definition'. This indicates the necessity to understand the ambit of these terms better to address the concern of their growth. Thus, there are no laws defining or providing for these concerns in the gaming sphere. Therefore, the White Paper does not significantly contribute to solving this issue of vagueness attached to bullying and extremism in the online gaming world.

[330] Home Office, 'Online Harms White Paper: Full Government Response to the Consultation' (n 150) 26.
[331] Ibid.
[332] Children's Commissioner, 'Gaming the System' (n 257) 4.

5.5 Gaps in current frameworks

(a) Gambling

The major gap in the Gambling Act regarding loot boxes and skins must be addressed. The definition of the term 'prize' needs to be reviewed and expanded to bring under its ambit items that may not have monetary value but, because of their non-monetary value, demonstrate gambling-like features and elicit gambling-like behaviours to qualify it as a phenomenon akin to gambling. In addition, the definition must be reformed to keep up with developing technologies. While the loot box feature is a pressing issue and a key tool used for the monetisation of games, the review of the legislation should not be restricted to it but rather should stay ahead of the curve by understanding and adapting to the rapid growth in gaming technologies.[333] One way of doing this is to keep the bigger picture in mind, i.e., the monetisation of games driven by profit-making motives of gaming companies at the cost of the 'best interests of the child', which would be prevention of addictive, gambling-like behaviour. Keeping in mind this overarching objective will guide legislative adaptation and development and 'future-proof legislation' [334] in accordance with the growth in gaming technology. Other jurisdictions in Europe, such as Belgium and the Netherlands, already regulate loot boxes under the ambit of the gambling framework.[335]

[333] Children's Commissioner, 'Gambling Act Review' (n 263) 5.
[334] Children's Commissioner, 'Gambling Act Review' (n 263).
[335] Children's Commissioner, 'Gaming the System' (n 257).

(b) Extremism

With regard to extremist content on online gaming platforms and associated chat platforms, there have been some efforts by the UK government to become involved in dialogues with the industry to combat this exploitative usage of the platforms, which is also a serious violation of the law.[336] As per Ukie, the UK's gaming trade body, there is an increased focus on 'sophisticated AI moderation tools and trained community managers' to make the platforms safer.[337] Such an attempt has been made by Roblox, which installed a 'fairly robust content moderation program' to remove inappropriate adult content as its majority audience is composed of children.[338] This program removes content that the company deems inappropriate from its platforms. However, there have been many complaints by content developers that their 'perfectly reasonable content' has been removed without any justification.[339] Such complaints can arise due to the subjectivity of what is deemed appropriate or inappropriate according to each company's policies. Thus, the question arises whether such practices and tools of online moderation can be codified into a legal mandate for the entire industry, considering the high costs of such technologies. Does a second practical question arise of determining (in) content appropriateness on these gaming platforms? A possible way forward is for specific design tools such as parental controls, screen time limits, chat group limits, etc., to only be determined after conducting an appropriate study and collecting adequate data that would provide an average standard at which these restrictions can be mandated, or at least identify the factors that should be considered when setting such standards.

[336] Carl Miller and Shiroma Silva, 'Extremists Using Video-Game Chats to Spread Hate', *BBC* (online, 23 September 2021) <https://www.bbc.com/news/technology-58600181>.
[337] Ibid.
[338] Copia Institute, 'Content Moderation Case Study: Roblox Tries To Deal With Adult Content On A Platform Used By Many Kids (2020)', *Techdirt* (4 June 2021) <https://www.techdirt.com/2021/06/04/content-moderation-case-study-roblox-tries-to-deal-with-adult-content-platform-used-many-kids-2020/> ('*Content Moderation Case Study*').
[339] Ibid.

One of the main problems that must be tackled with respect to combatting extremism in online gaming spaces is the lack of proper subcultural knowledge. It is also important to be a part of that culture to gain subcultural knowledge. Considering the extremely low levels of experience when it comes to 'prevent and counter violent extremism' (P/CVE) measures in the online gaming platforms, it is important for the organisations responsible for P/CVE measures to partake in these communities to understand the language, terminologies, and phrases that will help distinguish between dark-themed gaming terminologies and extremist content. It is not always straightforward to delineate the boundaries of extremist content. Even more so, it is difficult to implement a top-down approach to regulation in the gaming sphere. Therefore, it is important to tackle the issue by being 'on the ground' and a part of the platform, offering counter-narratives to extremist content, and the P/CVE organisations can do this.[340] The idea is to use the techniques of extremists to reinforce counter-narratives and positive alternative viewpoints to prevent the brainwashing of vulnerable children.[341] Drawing upon this idea, another possible tactic is an open conversation with children, just as the extremist groups do, except it would be for facilitating positive conversations rather than radical ones. [342] For example, the Dutch police's project 'Gaming with the police' provides children with the opportunity to game alongside the police.[343] The police personnel in this project do not jump into the warning-clad conversations regarding extremist content and the harmful influence of extremist groups but rather get involved in open conversations about the games and gameplay to foster a positive relationship with the children.[344] This way, trust and camaraderie are developed between the 'protectors' and the 'protected', which can be translated into more serious discussions whenever necessary.

[340] Schlegel (n 279) 14.
[341] Ibid.
[342] Ibid 15.
[343] Ibid.
[344] Ibid.

(c) Economic exploitation

Economic exploitation of children has evolved drastically from being limited to child labour and associated nuances to children being a target for, in digital gaming spaces, gambling-like features, in-app purchases, advertisements for in-game purchases, etc. Hence, this volution of the meaning of economic exploitation must be reflected in the legal framework. Further, not only the platforms where economic exploitation takes place have drastically changed, but the meaning of economic exploitation has because complicated as well. Gathering data about children through their chats and peer relationships in digital gaming platforms is one of the aspects through which economic exploitation is rampant. Digital gaming is one of the aspects of the digital environment that provides many ways for the economic exploitation of children. Hence, this must be taken into consideration in the legal framework. The GC also briefly touches upon the economic exploitation aspect without addressing the new angles in the digital sphere, especially relating to the gaming sphere.[345] Hence, acknowledging the evolution followed by a reflection of the same in the legal framework is necessary to tackle the economic exploitation of children.

5.6 Recommendations

(a) Changes in Legislation

Regarding the gaps in tackling the gambling-like features of digital games, there exists a window for including loot boxes within the ambit of the regulatory framework under the Gambling Act. Section 41 of the legislation provides for the liability of a person vis-à-vis gambling software, computer software used for remote gambling, unless used exclusively with a gaming machine.[346] In this case, if the algorithm or the software for loot boxes is included within this definition, then the person who provides for this software can be brought under the ambit of the regulatory framework of the Gambling Act.

[345] *General Comment No. 25* (n 192) 19.
[346] *Gambling Act 2005* (n 318) s 41.

Furthermore, specific design-related settings should be made mandatory across the industry in relation to loot boxes. Currently, in the UK, leading games have been made subject to certain measures such as probability disclosures[347] and default settings in games that provide the choice to the gamer to turn off, manage, or limit money spent.[348] Similarly, parental control tools such as limits on screen time are also employed by some of the major gaming consoles, including Xbox One and Nintendo Switch. However, there are no generally applicable standards for the industry as a whole, and therefore, there is a lack of uniformity and universality regarding such protective design or default features. Thus, specific regulatory frameworks setting standards with respect to, *among other things*, maximum daily spending, warnings regarding nudge techniques, additional warnings regarding in-game spending, parental controls and the provision of further digestible information to children must be formulated to achieve certainty, transparency and effective outcomes in terms of protecting children from developing harmful, gambling-like behaviours.

(b) Aid of Education

While specific legislative and technical solutions are important, certain generic solutions must be adopted for the wholesome prevention of online harm or the adverse effects of online gaming. Further, these solutions will also supplement the technical solutions provided above. The importance of merging online gaming with education cannot be overstated. Indeed, a strong analogy between digital gaming education and physical education (PE) can be drawn. As a widely accepted practice, children usually have dedicated classes to PE in schools. This is how physical games are integrated into the academic curriculum. Many aspects of the physical interaction, such as the rules of the games, conduct during the games, sportsmanship, fair play, anti-bullying, etc., are taught to children.

[347] Rob Davies, 'Video Game Loot Boxes Linked to Problem Gambling, Study Shows', *The Guardian* (1 April 2021) <https://www.theguardian.com/society/2021/apr/02/video-game-loot-boxes-problem-gambling-betting-children>.
[348] Ibid.

Similarly, considering that online games have become such a major part of children's lives and relationships, this must be reflected in their education. Dedicated classes on digital literacy can teach children acceptable behaviour and conduct with respect to other peers in the online gaming environment. They can also be taught the dangers that can come with online gaming to empower them to protect themselves from the potential harms arising from gaming platforms. Such integration of gaming and education will also help teachers and parents understand the gaming world's subcultural knowledge and the various dynamics that a child is faced with in navigating this digital space. This will ensure that children's interaction and engagement with these spaces occur in a meaningfully and effectively supervised manner without children feeling overly interfered with or restricted by authority figures. More specifically, in relation to gambling, children can be taught about the nuanced differences between gaming and gaming with gambling-like features. Indeed, education can be a vital instrument in bridging the existing legal gaps with knowledge and awareness gaps.[349]

6 Reporting to the Committee on the Rights of the Child

The UK is in a unique position as its reporting to the UN Committee on the Rights of the Child is composed of reporting by four countries: England, Wales, Scotland, and Northern Ireland.[350] The Joint Commissioner of these countries sends a report to the UNCRC to update on the implementation process of the Convention and the protocols.[351] The UK is due to update the UNCRC on implementing the 30 rights that it has identified in January 2022, followed by a further report in September 2022 with 'Concluding Observations'.[352] The UNCRC will also review the human rights situation vis-à-vis children in the UK in 2022. In 2020, the UK government submitted a report on children's rights in the light of COVID-19.[353]

[349] Lulu Freemont, 'The Rise of Skin Gambling: How Outdated Legislation Allows Thousands of UK Children to Gamble Online', *Parenting for a Digital Future* (17 April 2019) <https://blogs.lse.ac.uk/parenting4digitalfuture/2019/04/17/the-rise-of-skin-gambling-how-outdated-legislation-allows-thousands-of-uk-children-to-gamble-online/> ('The Rise of Skin Gambling').
[350] 'Report to the United Nations Committee on the Rights of the Child', *Children's Commissioner for England* (18 December 2020) <https://www.childrenscommissioner.gov.uk/report/report-to-the-united-nations-committee-on-the-rights-of-the-child/>.
[351] Ibid.
[352] 'Reporting on the UNCRC', *The Children and Young People's Commissioner Scotland* <https://www.cypcs.org.uk/rights/human-rights-monitoring/reporting-on-the-uncrc/>.
[353] Ibid.

(a) More and better data collection

The GC highlights that "regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives, evaluating its impact on their rights and assessing the effectiveness of State interventions."[354] The UK has also previously called for more data regarding children's rights.[355] Data collection offers a plethora of benefits, such as comprehensive data on mental and physical health, which can provide informed investment and regulatory decisions. However, data collection is a double-edged sword, and there are dangers in specific types of data collection in an under-regulated space, namely in the context of social media and Big Tech. Nevertheless, more data and more detailed research will encourage the identification of digital harm as a distinct issue to raise in the UK's reporting to the Committee on the Rights of the Child.

A learned reader would spot an allusion to digital harm in the report that briefly states:

> "Continue and strengthen preventive and protection measures to address the issue of harmful practices, including the collection of data, the training of relevant professionals, awareness-raising programmes, the provision of protection and care to the child victims and the prosecution of those found guilty of perpetrating such acts."[356]

The general understanding of the harmful practices is medical, such as genital mutilation or unnecessary surgeries and other procedures on intersex children. Therefore, it is not clear in the report whether the recommendation intends to cover the specific harmful practices of online service providers who process data.

[354] *General Comment No. 25* (n 2) 5.

[355] Committee on the Rights of the Child, *Concluding Observations on the Fifth Periodic Report of the United Kingdom of Great Britain and Northern Ireland* (No CRC/C/GBR/5, 12 July 2016) <https://digitallibrary.un.org/record/835015?ln=en>.

[356] Ibid.

(b) Sector-specific reporting

GC No. 25 deals with an extremely niche and technical area. It would take knowledge in science and technology and expertise in social science such as child psychology to ensure a wholesome approach to the vast array of issues under consideration. The online gaming system is rapidly growing with extremely advanced technology at the disposal of not only children but also groups that intend to violate children's rights and freedoms. Accordingly, we recommend one way of ensuring effective reporting is to deal with each issue separately and in detail rather than superficially touching on every issue related to children's rights in a single report. This will assist the UNCRC in comprehending better and reviewing countries' performance in the steps that have been taken in specific issue areas. Hence, it is suggested that the UK government's reporting regarding online harm should be contained in a separate report that exclusively reports on issues of concern in the digital gaming sphere. Moreover, as online gaming is extremely under-regulated, it also deserves exclusive focus to drive much-needed progress in ensuring that companies' profit motives do not compromise the best interests of children.

7 Recommendations and proposed solutions

7.1 Child impact assessments

Stakeholders have identified a concern that there is a lack of young persons' views in policymaking on issues that affect them.[357] This is a key reported issue in the UK's UNCRC Report.[358] As noted by the GC, "States parties should identify and address the emerging risks that children face in diverse contexts" by listening to the child's views "on the nature of the particular risks that they face." In addition, States should ensure that "digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services."[359]

[357] Children's Commissioner, *Life in Likes: Children's Commissioner Report into Social Media Use among 8-12 Year Olds* (4 January 2018) <https://www.childrenscommissioner.gov.uk/report/life-in-likes/>.

[358] Report on the Children's Commissioners of the United Kingdom and Northern Ireland to the United Nations Committee on the Rights of the Child (December 2020) available at< https://www.childrenscommissioner.gov.uk/wp-content/uploads/2020/12/cco-uncrc-report.pdf>

[359] *General Comment No. 25* (n 2) 3.

Therefore, we recommend that young people and parents alike be included to give feedback on the safe design of the platforms. In addition to tailoring safeguarding measures to those at risk of harm, participation and "the use of digital technologies can help realise children's participation at the local, national and international level."[360] That is, participation in platform design may help children realise that their online activities are not 'sheltered' because they only involve them. Children should be shown exemplar models of safeguarding notifications in those discussions, to assess whether they understand the purpose of the notification and can identify the key pieces of information. Experimentation can determine which colours, layouts, pictures, and text sizes are the most effective.

In the new Draft Online Safety Bill, risk assessment forms a major aspect of ensuring safety from harmful content in regulated services. While the risk assessment process and the factors to be considered for the same are comprehensive as they require an understanding of the demography of the service-users, etc., the assessment itself does not mention anything about children's participation directly. The assessments are to be done either by the regulator OFCOM or by the service provider (using their judgment).[361] However, it is recommended that children be active participants in this assessment to further their right to freedom of expression and right to be heard and ensure that the risk assessment is effective.

7.2 Child Rights by design

- Age Assurance: If a child attempts to recreate a social media account, they would have to put the email address of a parent or guardian, who could then approve or deny the account. Two links can be sent to the parent: one to confirm or deny the account and another to set the privacy settings. Suppose this child later wishes to change these settings instead of the Code's pop-up recommendation to seek guidance from an adult (which the child can swipe away). In that case, approval will need a PIN sent to the parent's email account or require facial recognition from an adult.

- Additionally, greater preventative action should be taken. For example, once the child attempts to resubmit their age, they are met with a series of 'bite-size' information blocks that explain what harm may arise if they try to access the platform. Assuming the user is under thirteen (Facebook's minimum age requirement), it can be gently explained that the platform is too old for them, like seeing a scary movie with too high an age rating. Children understand the concept of age-rated movies, so why not age-rated platforms? The platform may redirect them to speak to a trusted guardian or teacher about having a social media account.

[360] Ibid.
[361] *Draft Online Safety Bill* (n 149) clauses 7-8.

- An ‘opt-out’ to essential cookies for children by design. If a child decides to opt-in, an alert could be sent to the guardian email account, as previously mentioned, which would then require their approval. If the account is not linked to a guardian, adequate ‘bite-size’ explanations of the consequences of changing data collections should appear. The pop-up should contain a series of explanatory images accompanied by highlighted keywords and shorter sentences, which the child must individually click through before consenting. For younger users, real-world analogies may be helpful. For example, returning to the age-rated movie example, changing preferences may be accidentally harmful, confusing, or scary, like if they glimpsed a movie meant for adults.

- There should be a clear ‘unsubscribe’ feature for certain types of content, which means similar content will never be shown on the newsfeed again. It should be as easy as it is to unsubscribe from emails.

- Platforms can enforce a ‘respite’ period to prevent continuous usage. For example, if a child has been using a platform for over an hour or two, the platform can force them to take a break by remaining frozen or not refreshing for the allotted time. Every hour, there may be a mandatory respite. Or, for every two hours, there is a twenty-minute respite. A banner will arise that informs the child what is happening and why in a friendly manner: “Yikes! You’ve been online for two hours. You do this a lot, when was the last time you saw your friends? We will now take a break. Why don’t you do the same? Go to the toilet, maybe eat something.”

- YouTube recently changed the settings for Autoplay to turn it off by default for users aged thirteen to seventeen. This should be a design feature for all platforms, especially TikTok and Instagram,

- Young children need to be informed of the data profile built on their preferences and the consequences of the type of content they engage in. When interacting with inappropriate content, a series of notifications should arise that inform the child.

8 Conclusion

Children must not be stuck between their right to enjoy and access online spaces and the risks to their rights and freedoms when they do. The increasingly rapid digitalisation of children’s play environments, educational spaces, and decisions that affect their lives requires immediate and strong attention. To offer children the full realisation of their rights, governments around the world will need to establish clear and justiciable regulations to protect the next generation.

Here we demonstrate the current regulatory position regarding child rights and the digital environment across four key risk areas. This process reveals the positive and negative consequences of such legislation and the gaps that must be filled as governments seek to implement General Comment No. 25. In addition, we highlight opportunities for the protection of children by design and by default.

As lawmakers grapple with creating enforceable, justiciable and practicable regulation, they repeatedly encounter resistance from the industry that profits from the commercialisation of children's digital environment. Governments must find a clear path through such policy challenges to reduce negative outcomes for children overall. We have noted opportunities for improvement in the United Kingdom, which has the potential to lead the world in digital oversight.

Now is the time for action. Opportunities to further online protections are presented each day as the United Kingdom progresses in the network of legislation and policy design to improve outcomes for young people. Other countries will learn from such experiences, if designed well, to the benefit of children worldwide.