

OFCOM consultation: Protecting Children from Harms Online

August 2024

“Shaping the online world children and young people want and the online world they deserve.”¹

1. Summary

The Northern Ireland Commissioner for Children and Young People (NICCY) has long expressed concern about children and young people’s digital rights and the importance of aligning offline and online safeguarding laws and protections. The recent report funded by the Safeguarding Board NI (SBNI) and published by Stranmillis University College, Belfast clearly outlines how these rights are not limited to the right to freedom of expression (United Nations Convention of the Rights of the Child (UNCRC) Article 13), freedom of association (UNCRC Article 15), the right to privacy (UNCRC Article 16) and the right of protection from violence and abuse (UNCRC Article 19), the rights that this consultation document mainly focuses on.² The 6,481 children and young people who participated in this research spoke about, for example, the importance of the online world in relation to their right to play (UNCRC Article 31), to health and health services (UNCRC Article 24), right to education (UNCRC Article 28) and freedom of thought, belief and religion (UNCRC Article 14).

“Children and young people report a wide range of positive online experience and that being online is not a bolt-on to their lives; it is absolutely integral to how they live almost every aspect of their lives today.”³

We, as a society, have reached a point where governments, civil society, parents and carers, and regulators are all demanding a better deal for children online. To achieve this, children need recognised in the digital environment as autonomous human rights holders with agency and evolving capacities, with distinct rights, views and interests to those of adults.⁴ We will not shape the online world children and young people want and deserve

¹ 5Rights | Making Child Online Safety a Reality: Global Toolkit launched (5rightsfoundation.com)

² Purdy, N., Ballentine, M., Lyle, H., Orr, K., Symington, E., Webster, D., York, L., (2023) Growing Up Online: Children’s online activities, harm and safety in Northern Ireland – an Evidence Report. Belfast: Centre for Research in Educational Underachievement (CREU), Stranmillis University College / Safeguarding Board for Northern Ireland (SBNI)

³ Ibid., p.3

⁴ https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf p.57



without them and the ambition of the Online Safety Act 2023 and the associated Children's Codes won't happen without their full participation.

2. Summary of Recommendations

Recommendation 1: Ofcom undertakes a Child Rights Impact Assessment on the Children's Codes and ensures it is publicly available.

Recommendation 2: Ofcom requires online services to undertake child rights due diligence, to carry out Child Rights Impact Assessments and ensure they are publicly available.

Recommendation 3: Ofcom publishes its assessment of the equalities impact on children and young people as required by the Section 75 statutory duties of the Northern Ireland Act 1998, and any mitigations/ changes required.

Recommendation 4: Ofcom to publish a Children and Young People's version of the outcome of this consultation.

Recommendation 5: Ofcom should consult on its Children and Young People's Participation Strategy as a matter of urgency in relation to monitoring the impact of the Online Safety Act and its relationship with the NI Executive's Online Safety

Recommendation 6: NICCY urges Ofcom to explore its powers as a regulator and how it might enhance a child's rights approach in these Children's Codes.

Recommendation 7: Ofcom to publish its strategy for monitoring the impact of the Children's Codes on children and young people's lives.

Recommendation 8: Ofcom to consider the 5Rights Foundation's standards for effective age assurance.

Recommendation 9: Ofcom to consider a wider set of rights in their 'Rights Impact' assessment at the end of each section across the five Volumes.

Recommendation 10: We recommend that Ofcom consider using the '4 Cs' Framework when engaging with children and young people in relation to online harms.

Recommendation 11: Ofcom to include in their guidance on conducting risk assessments to include a comprehensive review against the full list of child rights in line with the UN Guiding Principles on Business and Human Rights (UNGPs) as well as the Children's Rights and Business Principles (CRBPs).



Recommendation 12: Ofcom to consider using the UNICEF modular Child Rights Impact Assessment toolkit.

Recommendation 13: Ofcom to establish and update a register of services operating in the UK.

Recommendation 14: Ofcom to develop child-friendly justice processes for children and young people to act on a breach of the duty to care.

3. Introduction

The Commissioner for Children and Young People (NICCY) was created in accordance with ‘The Commissioner for Children and Young People (Northern Ireland) Order’ (2003) to safeguard and promote the rights and best interests of children and young people in Northern Ireland (NI). Under Articles 7(2) and (3) of this legislation, NICCY has a mandate to keep under review the adequacy and effectiveness of law, practice and services relating to the rights and best interests of children and young people by relevant authorities. Under Article 7(4), NICCY has a statutory duty to advise any relevant authority on these matters.

The Commissioner’s remit includes children and young people up to 18 years or 21 years, if the young person is disabled or is care experienced. In carrying out his functions, the Commissioner’s paramount consideration is the rights of the child or young person, having particular regard to their wishes and feelings. In exercising his functions, the Commissioner considers all relevant provisions of the UNCRC. NICCY’s remit includes all reserved matters affecting children in NI. Online Safety is a multidimensional issue that relates to both the reserved matter of ‘Telecommunications’ but also, importantly, the devolved matters of safeguarding, education and policing in NI.

4. Children’s Rights Online

General Comment 25 (GC25) was adopted by the UN Committee on the Rights of the Child in 2021 and makes explicit for the first time that all children’s rights apply in the digital world. Those States who are signatories to the Convention will now have to report formally on the General Comments’ provisions. It holds that:

“The rights of every child must be respected, protected and fulfilled in the digital environment. Innovations in digital technologies affect children’s lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the Internet. Meaningful access to digital technologies can



support children to realize the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.”⁵

GC25 states that the following four principles provide a lens through which the implementation of all other rights under the UNCRC should be viewed. They should serve as a guide for determining the measures needed to guarantee the realisation of children’s rights in relation to the digital environment.⁶ Relevant Articles are as follows:

Article 9: Non-discrimination

The right to non-discrimination requires that States parties ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them.

Article 12: Best interests of the child

The best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context. The digital environment was not originally designed for children, yet it plays a significant role in children’s lives. States parties should ensure 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.

Article 14: Right to life, survival and development

Opportunities provided by the digital environment play an increasingly crucial role in children’s development and may be vital for children’s life and survival, especially in situations of crisis. States parties should take all appropriate measures to protect children from risks to their right to life, survival and development. Risks relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist. States parties should identify and address the emerging risks that children face

⁵ Para 4, General Comment 25 [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment | OHCHR](#)

⁶ tbineternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

in diverse contexts, including by listening to their views on the nature of the particular risks that they face.

Article 16: Respect for the views of the child

Children reported that the digital environment afforded them crucial opportunities for their voices to be heard in matters that affected them. The use of digital technologies can help to realize children's participation at the local, national and international levels. States parties should promote awareness of, and access to, digital means for children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed, so that they can be effective advocates for their rights, individually and as a group.

GC25 is clear that governments should review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention and the Optional Protocols thereto. Legislation should remain relevant, in the context of technological advances and emerging practices. They should mandate the use of child rights impact assessments to embed children's rights into legislation, budgetary allocations and other administrative decisions relating to the digital environment and promote their use among public bodies and businesses relating to the digital environment.⁷

The most recent Concluding Observations by the UNCRC for the UK and NI also referred to the importance of safeguarding children's rights in the now Online Safety Act. It stated that the State Party should adopt the Online Safety Bill and ensure that all laws and policies on the digital environment protect the rights, privacy and safety of children in the digital environment and from harmful content and online risks.⁸

The Council of Europe Strategy for the Rights of the Child (2022-2027)⁹ includes a focus on children's rights in the digital environment which is reinforced by the Recommendation

⁷ Para 23

internet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

⁸

internet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGBR%2FCO%2F6-7&Lang=en

⁹ Council of Europe Strategy for the Rights of the Child [1680a5ef27 \(coe.int\)](https://www.coe.int/t/e/children/strategy/1680a5ef27)



CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.¹⁰ The new Handbook for policy makers on the rights of the child in the digital environment completes these guidelines, by supporting policy makers in dealing concretely with the online rights and protection of children.¹¹ It assists with the development of national frameworks and policies and provides interpretative and practical guidance to ensure the respect of children's rights online.

The Council of Europe's Strategy specifically refers to the following set of rights from the UNCRC and European Convention on Human Rights (ECHR) and Sustainable Development Goals (SDGs):

Key UNCRC Articles were outlined as:

- Article 13 – Express themselves and seek information.
- Article 19 – Be protected from violence and abuse.
- Article 28 – Education; and
- Article 31 – Leisure and play.

Key ECHR Articles are:


- Article 3 – Not being subjected to torture or to inhuman or degrading treatment or punishment.
- Article 8 – Respect for private and family life.
- Article 10 – Freedom of expression.
- Article 14 – Prohibition of discrimination; and
- Article 2 of Protocol 1 – Education.

UN SDGs Goals:

- Quality of Education.

¹⁰ 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 [16808d881a \(coe.int\)](#)

¹¹ Handbook for policy makers on the rights of the child in the digital environment [1680a069f8 \(coe.int\)](#)



- Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women and girls.
- Significantly increase access to information and communication technology and strive to provide universal and affordable access to the internet; and
- End abuse, exploitation, trafficking and all forms of violence against and torture of children.


The Strategy then focuses on these challenges that are relevant to the development of these Children's Codes:

- Digital services or products may not be designed to meet the needs or uphold the best interests and the rights of children, including their freedom of expression, their right to information and their safety.
- Children access or share inappropriate or harmful content.
- Children suffer from online bullying and hate speech, including by peers, from interference with their right to privacy and personal data protection, from information disorders as well as from overuse or even online addiction, leading to isolation and lack of physical activity and related health and mental health issues.
- The risks and opportunities posed by the use of artificial intelligence systems are yet to be analysed.
- Digital citizenship and media education is still not sufficiently provided for children, carers, professionals and volunteers working with children. Children are aware of this gap and perceive a need to be engaged more proactively in developing and delivering training and education to different target groups, as well as in assessing training and education needs in this field; and
- Child participation in the regulation, design and innovative use of the digital environment and technology is limited.

The Council of Europe's Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment also offer further guidance.¹²

Children's experiences online are not limited to products and services directed at them or even accessed by them. There are many services and situations that impact on children without their direct participation, for example, facial recognition technology in public

¹² [Guidelines to respect, protect and fulfill rights of the child \(Council of Europe\) 101818GBR_CM Rec 2018 7.pdf](#)



places, predictive policing technology, technology used by government to assess need or algorithms in exam grading. Technological services such as these that engage children without their participation often affect them in ways they may not know.¹³ Whilst the scope of these Children's Codes is limited to user-to-user services and search services it is critical that a child's rights approach is front and centre in all digital products and services. Young people involved in the 5Rights Foundation have considered and recommended how this should be done incorporating the UNCRC, ECHR and SDGs:

1. Protect children's rights online.
2. Make rules that support children's rights online. Ensure that everyone understands the rules, including government officials, businesses, parents, teachers and children themselves.
3. Listen to children when they have a problem.
4. Stop businesses putting profit above children's rights.
5. Make sure that there are consequences for organisations or people who break the rules.
6. Make sure children know and understand what action has been taken.¹⁴

These are the outcomes the Children's Codes need to achieve. Ofcom's limited focus on children and young people's rights is a missed opportunity to ensure that the draft Codes are demonstrably compliant with children's rights.

Our concern with regards the absence of any CRIAs being undertaken and a wider analysis of the impact of these draft Children's Codes on all rights is compounded by the lack of any indication that Ofcom, as a public authority, has undertaken an equalities impact assessment as required by the Section 75 statutory duties of the Northern Ireland Act 1998 and identified the impact of these proposals on children and young people, as well as any associated consultation.

Recommendation 1: Ofcom undertakes a Child Rights Impact Assessment on the Children's Codes and ensures it is publicly available.

Recommendation 2: Ofcom to require online services to undertake child rights due diligence, to carry out Child Rights Impact Assessments and ensure they are publicly available.

¹³ https://5rightsfoundation.com/uploads/Ambitions_for_the_Online_Safety_Bill.pdf

¹⁴ [In our own words- young people's version of GC25.pdf \(5rightsfoundation.com\)](#)



Recommendation 3: Ofcom publishes its assessment of the equalities impact on children and young people as required by the Section 75 statutory duties of the Northern Ireland Act 1998, and any mitigations/ changes required.

5. Children and Young People’s Participation

NICCY recognises the significant body of work that Ofcom has conducted over the last two years with children and parents. 15,000 children had been surveyed and 7,000 parents.¹⁵ The outcome of this research shows a bleak picture, with children being exposed to violent content, suicide, self-harm, ever more violent and extreme. Ofcom’s research found that 51% of children 8-12 already have a social media account and one-fifth of children aged 8 to 17 have accounts identifying them as over-18.¹⁶ Of children aged 5 to 7, who are increasingly present online – a third use social media unsupervised, and a growing number have personal profiles.¹⁷

NICCY is concerned that there was no children and young people’s version of this consultation document published. Given the length of the consultation document {with more than 1,200 pages), and the language used within it, it is not easily accessible for children and young people, let alone their families, carers or wider civil society. We appreciate that Ofcom has and is considering how to support the participation of children and young people but out of the whole document there are five pages at the end which specifically outlines Ofcom’s thinking on this. NICCY would encourage Ofcom to publish a children and young people’s version of the outcome of this consultation, ensuring that their views and experiences are reflected adequately.

NICCY’s Youth Panel met with Almudena Lara, Policy Lead for the Protection of Children and valued this engagement. Our response is informed by this conversation, ongoing conversations with our Youth Panel and responses to the surveys we sent out.

The importance of consultation was outlined by a NICCY Youth Panel member, as follows:

“Regardless of how many ‘checks’ companies and organisations put in place, or say they will, online safety may never reach the level we need it as long as young people are not consulted, and society informed.” (NICCY Youth Panel Member)

¹⁵ [Research, statistics and data - Ofcom](#)

¹⁶ [A third of children have false social media age of 18+ - Ofcom Encountering violent online content starts at primary school - Ofcom](#)

¹⁷ [A window into young children’s online worlds - Ofcom](#)



The Consultation document also states that Ofcom have commissioned Revealing Reality to speak with children from across the UK to find out what they think about the draft Children's Safety Codes with the objective of engaging between 100-120 children aged 8-17. It is our understanding that Revealing Reality and Ofcom are developing child-friendly materials about the codes and designing workshops to share these materials, which is welcome. The document concludes that this will allow children's views to be fed into the consultation process. However, we have been unable to find any details on these workshops including the child-friendly materials or workshop session plans.

NICCY also understands that a Strategy is being developed to work with children and young people in monitoring the impact of the Online Safety Act and the Children's Codes which includes:

- A Children's Online Research Panel which will facilitate ongoing engagement with children in a variety of ways.
- A Children's Online Safety Tracker to monitor risks and harms, and attitudes and experiences of online safety measures.
- An Online Passive Measurement tool to better understand the online platforms and services being used by children; and
- Further behavioural trials among under 18s to better understand how to positively influence children's decision making online.¹⁸

We understand that this research will be complemented with direct work with regulated service providers to help Ofcom understand, assess, and drive improvements and understand what measures might work to protect children from harm.

We would have liked to have seen further details on this Strategy, associated action plans, the resources allocated, and where it 'sits' within Ofcom's wider work in order to fully respond to this consultation. NICCY would welcome more information on how it will tie in with the NI Executive's Online Safety Strategy and Action Plan.¹⁹

We also must acknowledge that adults can have conscious and unconscious biases and assumptions about children and their use of technology; without children's full

¹⁸ [Protecting children from harms online - Volume 5: What should services do to mitigate the risks of online harms to children? \(ofcom.org.uk\)](#) p.15

¹⁹ [Online Safety Strategy and Action Plan | Department of Health \(health-ni.gov.uk\)](#)



participation, voices and insights adults will never be able to ensure that the online world is one that young people want and deserve.

Recommendation 4: Ofcom to publish a Children and Young People’s version of the outcome of this consultation.

Recommendation 5: Ofcom should consult on its Children and Young People’s Participation Strategy as a matter of urgency in relation to monitoring the impact of the Online Safety Act and its relationship with the NI Executive’s Online Safety Strategy and Action Plan.

6. Summary of evidence of Children’s Experience in NI of Online Harms

Two important streams of research work in relation to young people’s digital rights and online safety have been undertaken by the SBNI and by The Executive Office (TEO) to inform the Online Safety Strategy and Action Plan. We summarise some of the relevant findings below.

The ‘Growing Up Online: Children’s online activities, harm and safety in Northern Ireland – an Evidence Report’ was commissioned by SBNI to inform the delivery of actions associated with the NI Executive’s five-year ‘Keeping Children and Young People Safe: An Online Safety Strategy’.²⁰ This report draws together research from a survey of 6,481 children and young people aged 8-18, and focus groups and interviews with 95 participants including children and young people in mainstream primary and post-primary schools, special schools and youth club settings, as well as parents/carers, teachers/school leaders, and professionals working in the field of online safety. It found clear evidence that around 1 in 5 children and young people (20% of 8-13 year olds and 18% of 14-18 year olds) have experienced something nasty or unpleasant happening to them online over the past couple of months, most commonly on social media app. Girls are much more likely to experience something nasty or unpleasant online, both among the younger cohort (23% girls vs 17% boys) and the older cohort (20% girls vs 15% boys).

There were a number of important findings with relevance to the Children’s Codes and their potential impact on children and young people in NI.

²⁰ [Online Safety Strategy and Action Plan | Department of Health \(health-ni.gov.uk\)](#)

Cyber Bullying

Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person. A total of 12.89% in the 8-13 year old cohort reported that “someone was mean to me online”.²¹ Upon further analysing this subgroup it was found that the majority of those who reported being cyberbullied were girls (56.8%) compared to a lower incidence among boys (39.8%).²² In terms of the frequency of the behaviour, 44% reported that it had happened three times or more in the past couple of months. The two most commonly cited reasons for cyberbullying among this younger cohort were “because of a fallout with friends” (37.7%) and “because of the way I look” (26.8%), with much lower numbers citing identity-based motivations such as family background (6.3%), gender (5.5%), religion (5.5%), race (3%), SEN (2.4%) and care status (1.6%).²³

The majority of 8-13-year-olds reported that the cyberbullying had taken place on social media sites (54.6%), followed by on a gaming site or console (30.4%) or on a group chat e.g. WhatsApp (27.8%) with fewer reporting that it had taken place via direct message (15%). In the majority of cases, the cyberbullying had been perpetrated by “a friend or other young person you know” (61.7%), with only a third reporting that it had been carried out by a stranger (37.1%).²⁴

Participants were asked whether they had reported the bullying. Of those who had indicated that they had experienced cyberbullying, just under half (46.6%) indicated that they had reported it, while 53.4% had not reported it. Girls (53.3%) were much more likely than boys (38.4%) to report their cyberbullying experiences. This correlates with Ofcom’s own research.²⁵ When asked to whom they had reported the cyberbullying, the two most cited responses were “I told a friend” (44.6%) and “I told a parent/carer/ other adult in the family” (42.2%).²⁶

In the survey questions for the older cohort of 14-18-year-olds, there were 16 different negative online experiences provided as options for the young people to choose from, not all of which could be described as cyberbullying behaviours. The cyberbullying sample is

²¹ [Spotlight Report on Cyberbullying \(safeguardingni.org\)](#)


²² Ibid.,

²³ Ibid., p. 5

²⁴ Ibid

²⁵ [Protecting children from harms online - Volume 3: The causes and impacts of online harms to children \(ofcom.org.uk\)](#) p.126.

²⁶ Op. Cit., p.6



focused on eight of those 16, subcategories. All participants in the sub-sample experienced one or more of these types of online bullying:

- Mean or nasty comments were made about me or sent to me (69.5%).
- Lies or rumours were told about me (51%).
- Embarrassing photos or videos of me were edited, posted, tagged, or shared without my permission (32%).
- I was threatened (26.3%).
- I was excluded from an online group (24.5%).
- Someone tried to blackmail me (19.5%).
- Personal information was shared about me without my permission (19%); and
- My personal account was hacked (11.7%)²⁷


When analyzed further by gender there were the following findings:

- Girls were more likely than boys to report that “mean or nasty comments were made about me or sent to me” (70.9% vs 63.6%), and more likely to report that “lies or rumours were told about me” (56.8% vs 45.7%) and more likely to report that “I was excluded from an online group” (27.1% vs 19.9%).
- Boys were more likely than girls to report that “someone tried to blackmail me” (21.2% vs 16.1%), boys were more than twice as likely as girls to report being threatened online (35.8% vs 17.6%) and were almost three times more likely than girls to report that their account had been hacked (17.2% vs 6.5%).
- While the numbers were often small, there appears to be a higher incidence of cyberbullying among those 14-18 year olds who identified as gay/lesbian or bisexual rather than heterosexual. For instance, a higher percentage of gay/lesbian (77.3%) and bisexual (72.4%) rather than heterosexual (68.2%) young people reported that “mean or nasty comments were made about me or sent to me” over the past couple of months. Similarly, when asked if they had been threatened, incidence was much higher among those who identified as bisexual (37.9%) and gay/lesbian (27.3%) compared to those who identified as heterosexual (21.6%).²⁸

As with the younger cohort, the two most commonly cited reasons for the cyberbullying among this older cohort were “because of the way I look” (33.1%) and “because of a fallout

²⁷ Op. Cit., p. 7

²⁸ Op, Cit., p. 7



with friends” (32.6%), with much lower numbers citing identity-based motivations such as gender (13%), sexuality (11.2%), family background (9.6%), religion (6.5%), SEN (5.7%), race (4.4%) and care status (3.1%).²⁹

Compared to 8-13 year olds, an even greater majority of the 14-18 year olds reported that the cyberbullying had taken place on social media sites (80.2%), followed by much lower but very similar incidence through a group chat e.g. WhatsApp (17.7%), via direct message (17.4%) or on a gaming site or console (17.2%). Among this older cohort compared to the younger cohort, there was a higher reported incidence of perpetration by someone they didn't know. Among 14-18 year olds, almost half (49%) reported that they had been cyberbullied by someone they didn't know, but they were still more likely to report that the cyberbullying had been carried out by a friend or another young person they knew (58.3%).


The 14-18 year old participants were also asked whether they had reported what had happened. Of those who had indicated that they had experienced cyberbullying, less than a third (31%) indicated that they had reported it, while more than two thirds (69%) had not reported it. This level of reporting was thus much lower than among the younger cohort. Girls (34.7%) were much more likely than boys (24.7%) to report their cyberbullying experiences. When asked to whom they had reported the cyberbullying, the two most commonly cited responses were once again “I told a friend” and “I told a parent/carer/other adult in the family” but within these instances the older cohort were more than twice as likely to tell a friend/friends (53.6%) than a parent/carer/other adult in the family (23.4%).³⁰

The focus group sessions brought out issues such as young people experiencing behaviour such as trolling and catfishing, and experiences by teachers of having to deal with very serious incidents, sometimes requiring the involvement of the police. Such incidents were reported to have very significant emotional impact on the children and young people concerned, although it was striking in some of the focus group interviews how the young people appeared to accept a certain level of risk and danger online and appeared confident in dealing with such incidents.

Key issues of relevance to the Children's Codes are the gender and age differentials with regards to reporting behaviours in relation to cyber bullying and the need to upskill parents, families and young people as young people are more likely to report to family and friends. Interestingly the extent of parental supervision and involvement can also be influenced by

²⁹ Op. Ci., p.8

³⁰ Op. Cit. P.9



their child's gender with girls who had been cyberbullied more likely to report higher levels of parental supervision than boys. ³¹

Parents and Carers

One of the most significant findings in the research related to levels of parental engagement in their children's online activities. ³² In particular, children and young people were asked to rate how interested their parents were in what they were doing online. Among both age cohorts (8-13 and 14-18) levels of parental interest, as perceived by their children, were low, and were especially low in respect of the older cohort (14-18).


For instance, among the younger cohort (8-13), just one in six respondents reported that their parents were 'very interested' in what they were doing online. Most felt that their parents were 'a little interested' while almost one in five claimed that their parents were 'not at all interested'. Among the older cohort (14-18), reported levels of parental interest were lower still. Less than one in ten respondents reported that their parents were 'very interested' in what they were doing online. Again, just over half felt that their parents were 'a little interested' leaving just over a third of young people claiming that their parents were 'not at all interested'. Perceived parental interest data were also analyzed in relation to gender. For both age groups, girls were more likely to report higher levels of parental interest than boys. ³³

The qualitative evidence through interviews and focus groups demonstrated how interested and concerned parents are. It was apparent that parents who have voiced their fears and described very clearly how interested they are in their child's online activity, often fail to avail of opportunities to become more informed and connected to their children when offered to do so. Teaching professionals reported very little engagement with parent evenings and training events, both in-person and online. ³⁴ Interestingly, one of the questions asked to children and young people related to who, in their opinion, is responsible for improving the safety of young people online. For both age groups, parents/carers were the most popular response.

³¹ [Spotlight Report on Parents and Carers \(safeguardingni.org\)](#) p.3

³² [Growing Up Online | Spotlight on Parents and Carers - Safeguarding Board for Northern Ireland \(safeguardingni.org\)](#)

³³ [Spotlight Report on Parents and Carers \(safeguardingni.org\)](#) p.9



Among the 8-13 group nearly three quarters believed that online safety is the responsibility of parents/carers. This was followed by schools, government and social media companies. Nearly a quarter believed that youth clubs/organisations and phone companies should make the internet safer for young people. The results were slightly different for the 14–18 year olds. Although almost two-thirds of the older cohort also felt that online safety is the responsibility of parents/carers, the lower rankings differed: among 14–18 year olds, parents/carers were followed by social media companies, schools and government. The least common responses included phone companies and youth clubs/organisations.³⁵ This has implications with regards to the monitoring of the impact of the Online Safety Act from young people’s perspectives.

Violence against women and girls

In 2021, the NI Executive directed that a Strategy to *End Violence Against Women and Girls (EVAWG)* be developed, with TEO leading on this whole of government, whole of society approach.³⁶ *‘It’s Just What Happens’ Girls and Young Women’s Views and Experiences of Violence in Northern Ireland*’ was one of the research reports produced.³⁷ Online misogyny was raised in the focus groups as one of the two most prevalent forms of violence experienced by girls and young women.

The normalisation of such behaviours reinforced across the offline and online worlds with little belief in the systems of reporting and that the online world ‘doesn’t matter as much’ or that there’s nothing that can be done, especially if that person is residing in a different jurisdiction. Discussions demonstrated how offline and online worlds interconnect reinforcing negative gender messages, objectification and a general lack of respect for women. Given that consequences are delayed, minimal or short-term young women felt they had no recourse other than to simply ignore or tolerate.³⁸

While online platforms were reported as useful space for learning about violence many of the participants in the research considered them also to be a place where violence and sexism were exposed and reproduced. This included: misogyny; receipt of graphic images and texts; requests for naked images; unsolicited ‘friend requests’; blackmail; constant pressures and expectations relating to female bodies.

³⁵ Op. Cit., p. 9

³⁶ [Ending Violence Against Women and Girls | The Executive Office \(executiveoffice-ni.gov.uk\)](#)

³⁷ [Ending Violence Against Women and Girls | The Executive Office \(executiveoffice-ni.gov.uk\)](#)

³⁸ [IT’S JUST WHAT HAPPENS’ Girls and Young Women’s Views and Experiences of Violence in Northern Ireland \(executiveoffice-ni.gov.uk\)](#) p.8.

Associated with this online climate of sexism and objectification of female bodies, some young women spoke of the unrealistic expectations they felt as a result of pervading messages about appearance, lifestyle and stereotypical gendered expectations in online forums and chat rooms.³⁹

The belief that ‘you have do it yourself’ may reflect the experience that a significant amount of online harms and violence is perpetrated via social media sites, and that these have so far largely failed to address this and protect users from online abuse with the only options to ‘block’, ‘delete’ or ‘ignore’.⁴⁰

This research clearly speaks to the safety measures being proposed by Ofcom including more effective content moderation, providing young people with information, tools, and support and ensuring that reporting and complaints functions are easy to use and most importantly, effective.

7. Comments on Each Volume

Volume 1

Ensuring a children’s rights-based approach.

NICCY welcomes the section on Human Rights and the commentary on UNCRC and GC25.⁴¹ We are however very disappointed that the wording of the UNCRC was not directly incorporated into the Online Safety Act, as was stated:

“Rather than making direct reference to the UNCRC (or General comment No. 25), we consider and reference the relevant statutory duties in the Act and impacts on ECHR rights, in line with the applicable requirements under UK domestic law, which encompasses and reflects relevant aspects of the UNCRC. In this way, our approach also encompasses, and is consistent with, relevant aspects of the UNCRC and General Comment 25, including in giving particular weight to the importance of the best interests of children in deciding on our proposals.”⁴²

³⁹ IT’S JUST WHAT HAPPENS’ Girls and Young Women’s Views and Experiences of Violence in Northern Ireland (executiveoffice-ni.gov.uk) p.36

⁴⁰ IT’S JUST WHAT HAPPENS’ Girls and Young Women’s Views and Experiences of Violence in Northern Ireland (executiveoffice-ni.gov.uk) p.64.

⁴¹ [Protecting children from harms online - Volume 1: Overview, scope and regulatory approach \(ofcom.org.uk\)](http://ofcom.org.uk), Para 2.38, p.14

⁴² [Protecting children from harms online - Volume 1: Overview, scope and regulatory approach \(ofcom.org.uk\)](http://ofcom.org.uk) Para 2.49 p.16

As a signatory to the UNCRC, the government should have ensured that the Online Safety Act formally recognised GC25 on children’s rights in relation to the digital environment. As previously discussed, the consequences of this are that the totality of children’s digital rights are not front and centre of these Children’s Codes.

NICCY urges Ofcom to explore its powers as a regulator how it might enhance a child’s rights approach in these Children’s Codes. For example, GC25 recommends the following in relation to CRIAs and safety by design industry standards:

“38. States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children. They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

39. In addition to developing legislation and policies, States parties should require all businesses that affect children’s rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child. They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service.”⁴³

Strengthening a rights-based approach would lend itself to the intent of the Online Safety Act and these Children’s Codes: to embed safety protections from the outset and ensure that the rights of children and young people are at forefront of design.

The impact of the ‘attention economy’

The ‘attention economy’ has generated huge revenues for social media platforms. Social media platforms Facebook, Instagram, Snapchat, TikTok, X, and YouTube collectively derived nearly \$11 billion in advertising revenue from U.S.-based users younger than 18 in 2022.⁴⁴ The 2023 Harvard Study was the first to offer estimates of the number of youth users on these platforms and how much annual ad revenue is attributable to them.

⁴³ General Comment 25

tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

⁴⁴ [Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model | PLOS ONE](#)



According to the research, YouTube derived the greatest ad revenue from users 12 and under (\$959.1 million), followed by Instagram (\$801.1 million) and Facebook (\$137.2 million). Instagram derived the greatest ad revenue from users ages 13-17 (\$4 billion), followed by TikTok (\$2 billion) and YouTube (\$1.2 billion).

The researchers also calculated that Snapchat derived the greatest share of its overall 2022 ad revenue from users under 18 (41%), followed by TikTok (35%), YouTube (27%), and Instagram (16%).⁴⁵ These figures demonstrate that it's not that children and young people haven't been at the forefront of the minds of many companies but that they have prioritised profit over rights.

“Young people are being failed on the internet. It is profits over protection, time and time again. We deserve better.” (NICCY Youth Panel Member)

A systems-based approach to regulation requires adherence to rights from the outset rather than dealing with problematic content once it's posted, which seems to be the main focus of the more than 40 safety measures as outlined in Volume 5. Children and young people are disproportionately affected by the risks of the digital world, given both their developmental vulnerabilities and their status as 'early adopters' of emerging technologies. They are 'canaries in the coal mine for threats to us all.'

Another challenge with the Children's Codes is balancing reduction in harms with the opportunities and benefits for children and young people in accessing online platforms and enabling their rights, for example, to education, play, right to be heard, access to information, and health. There is a very careful balancing act to be achieved in the proposed use of age verification and age assurance technologies if the result is not simply to be cutting young users off from the services and practices they value so highly.”⁴⁶

NICCY agrees with the principle of proportionality as expressed in Volume 1 in that Ofcom must have regard to the need for a higher level of protection for children than for adults, while ensuring children retain the benefits of being online. In addition, a 'one-size-fits all' approach will not work; however, this cannot be used as reason for services to refuse to take steps to protect children because of costs or practicalities. As Baroness Ritchie of

⁴⁵ [Social media platforms make \\$11B in ad revenue from U.S. teens — Harvard Gazette](#)

⁴⁶ [OII | Safer Internet Day 2023 – OII Director Victoria Nash & OII Visiting Policy Fellow, Lisa Felton, give their perspective on how to make the online world safer for children \(ox.ac.uk\)](#)



Downpatrick has commented, we do not take a proportional approach to the sale of alcohol, or cigarettes and we don't treat a corner shop differently from a supermarket. 48

We also are mindful of the debate in the House of Lords during the passage of the Online Safety Act and the below intervention by Lord Russell of Liverpool on the danger of companies remodeling their services to avoid regulation.

“In particular, we have tabled these amendments because one of the possible unintended consequences of the well-meaning and serious attempts by all of us to protect children better is that some of these companies and platforms may decide that having children access some of their services is too much bother. They may decide that it would be simpler to find means to exclude them completely because it would be too much trouble, money or regulatory hassle to try to build a platform or service which they know children will access, as that will impose a serious obligation on them for which they can be held legally accountable. That would be an unintended consequence. We do not want children locked out of services which are essential to their development, education and self-expression.”⁴⁷

These Codes and Guidance will need to be updated on a regular basis as technology evolves and changes and new evidence emerges of risks to young people. In this regard, NICCY would have welcomed more details on how Ofcom will monitor and measure the impact of these codes on outcomes for children and young people as set out for example as below.

Recommendation 6: NICCY urges Ofcom to explore its powers as a regulator and how it might enhance a child's rights approach in these Children's Codes.

Recommendation 7: Ofcom to publish its strategy for monitoring the impact of the Children's Codes on children and young people's lives.

Volume 2

We agree that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance. We welcome the set of standards developed by the 5Rights Foundation which go further than the four standards used by Ofcom: technical accuracy, robustness, reliability, and fairness.

The 5Rights Foundation set out their standards in their paper '*But How Do They Know It Is A Child?*'. These are privacy-preserving, rights-respecting, proportionate to risk and purpose,

⁴⁷ [Online Safety Bill - Hansard - UK Parliament](#)



easy for a child to use, accessible and inclusive, and enhances a child’s experience, rather than merely restricts it, offering a high level of security, transparency, accountability, and clear routes to challenge and redress.⁴⁸ We recommend that Ofcom considers these wider set of standards.

We also agree that given the clear intention of the Online Safety Act to ensure that regulated services are designed and operated in a way that secures a higher standard of protection of children than for adults, it was not the intention of Parliament that the concept of a “significant number of children” within the meaning of the Act should require the number in question to be a large or substantial number, either in absolute terms or as a proportion of child users compared to the overall user base. Instead, we agree that this term should be understood as indicating that the number of children on the service is material in the context of the service in question. A single numerical threshold might lead to services that potentially pose a very serious risk of harm to a relatively small number of children concluding that they do not have to abide by the child safety duties.

The factors the service providers need to consider to decide whether a child user condition is met seem comprehensive focusing on the four categories of:

- Whether the service provides benefits for children.
- Whether the content on a service appeals to children.
- Whether the design of the service appeals to children; and
- Whether children form part of a service’s commercial strategy.

We acknowledge the ‘rights impact’ section that Ofcom follows throughout these five volumes with a focus in the main on the ‘interference’ of their proposals with users’ (both children and adults) or services’ freedom of expression or association rights.

We would recommend that Ofcom explore whether a broader range of children’s rights could be assessed at these junctures following the framework of a child rights impact assessment evaluating the impact of the proposals against children’s rights as defined in the UNCRC, and other internationally accepted human rights and child rights instruments.⁴⁹

Recommendation 8: Ofcom to consider the 5Rights Foundation’s standards for effective age assurance.

⁴⁸ [5Rights Foundation](#)

⁴⁹ [Child Rights Impact Assessments in Relation to the Digital Environment.pdf \(unicef.org\)](#)



Recommendation 9: Ofcom to consider a wider set of rights in their ‘Rights Impact’ assessment at the end of each section across the 5 Volumes.

Volume 3

Online crimes

Whilst this consultation is not focused on illegal harms it is worth noting the statistics on online crime. In 2022/23, 5% of all crimes recorded by the PSNI took place online, with three such offences recorded per 1,000 population. Victims aged under 18 were most likely to be victims of malicious communications, harassment or sexual activity offences with an online motivation while those aged 18+ were most likely to be victims of malicious communications, harassment or blackmail. Females were most likely to be victims of malicious communications, harassment or sexual activity, with males most likely to be victims of malicious communications, harassment or blackmail.⁵⁰

In relation to sexual grooming offences against children in NI, the PSNI have stated that the first sexual grooming offences were recorded in 2004/05 and the offence of sexual communication with a child which was introduced in 2015/16. While the overall classification increased by 152 offences from 34 in 2016/17 to 186 in 2017/18, much of the increase was attributed to the activity of Online Child Sexual Abuse Activist Groups (more commonly known as ‘paedophile hunters’ who engage by posing as a child under 16). This activity did not continue to the same extent into 2018/19, and the number of sexual grooming offences reverted to levels seen prior to 2017/18. There were 22 offences of sexual grooming and 198 offences of sexual communication with a child recorded in 2022/23, accounting for 10% and 90% of offences recorded in this classification respectively.

The connection between ‘legal’ harms to children and young people leading to ‘illegal’ harms is well demonstrated in this consultation in the evidence that suggests that perpetrators of child sexual exploitation and abuse are deliberately targeting children. Child sexual exploitation and abuse perpetrators posing as ‘anorexia coaches’ with

⁵⁰ See: [Trends In Police Recorded Crime 1998-99 to 2022/23 \(psni.police.uk\)](https://psni.police.uk)

children with experience of an eating disorder connecting with these ‘anorexia coaches’ becoming at greater risk of harm of sexual abuse.⁵¹

NICCY recognises that the assessment of the causes and impacts of online harms in this section draws from a significant body of work including Ofcom-commissioned research with parents and young people alongside 500 quality-assured sources that represent children’s own voices, as well as parents, carers, practitioners, and other experts.

The ‘4C’s’ framework

The ‘4C’s’ framework classifies online risks as content, contact, conduct and contract (sometimes referred to as commercial) risks. The framework has been widely adopted around the world, most recently by the Organisation for Economic Co-operation and Development (OECD), the European Commission, and the United Nations.⁵²

It recognises that new technology can often hurt the most vulnerable members of society first and it provided an accessible way for our NICCY Youth Panel to consider online harms. We recommend that Ofcom consider its use when engaging with children and young people on the causes and impacts of online harms.

Overall, NICCY agrees with Ofcom’s assessment on the causes and impact of online harms. One of the areas specifically highlighted by our NICCY Youth Panel was the impact of addiction to the digital environment and technologies, including virtual reality. This is also highlighted in the Council of Europe’s Strategy for the Rights of the Child.⁵³ Several members of our Youth Panel shared their concerns and experiences around this including

⁵¹ 7.3.68 There is evidence to suggest that perpetrators of child sexual exploitation and abuse (‘CSEA’) are deliberately targeting children with the intent of sexual exploitation. An exploratory study into the vulnerability of children to human trafficking reported on a number of criminal and investigative journalism cases (across the UK, the Netherlands and Germany) where CSEA perpetrators were posing as ‘anorexia coaches’ to exploit sexual images and acts from young women and girls.⁴²⁷ Direct messaging was used to build a relationship between the ‘coach’ and child or young adult, and the dependency and loyalty they felt towards their ‘coach’ was noted as contributing to the exploitation. Children with experience of an eating disorder who connect with ‘anorexia coaches’ are therefore at greater risk of harm of sexual abuse. Refer to the Illegal Harms Register within our Illegal Harms Consultation (see CSEA section). [Protecting children from harms online - Volume 3: The causes and impacts of online harms to children \(ofcom.org.uk\)](#) p.93

⁵² [ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf](#) p.8

⁵³ COUNCIL OF EUROPE STRATEGY FOR THE RIGHTS OF THE CHILD (2022-2027) [680a5ef27 \(coe.int\)](#) p.30



their lack of awareness in regard to whether there existed community-based support services for the young people and families concerned.

The NICCY Youth Panel also felt that adults and service providers did not understand the extent of how their online and offline worlds are so connected for better or for worse and that risks are also dependent on the personal experience and perception of risk and how often they are exposed to it.⁵⁴

“Sometimes offline threats force children and young people into online harms.”
(NICCY Youth Panel)

From the outset, it is vital to distinguish between online risk and harm. Conceptually, risk is the probability of harm, while harm includes a range of negative consequences to the child’s emotional, physical or mental wellbeing.⁵⁵ For example, exposure to pornography poses a risk to a child, but it is not a certainty that there will be harmful consequences. Harmful impacts depend on the risk, on the design, regulation and management of the digital environment and on the circumstances of the young person.⁵⁶

This is recognised by Ofcom with the presence of abuse and hate content in children’s online lives sometimes affecting the volume of offline incidents of abuse.⁵⁷

The use of ‘code words’ online that mask harms were also brought up by our Youth Panel. They gave examples such as ‘I ran out of shampoo and conditioner at the one-time’ masking posts about suicidal thoughts or ‘grippy socks’ for time in residential care. As Ofcom notes, children can search for code words as opposed to explicit terms to evade detection or censorship which then be disseminated by recommender systems.⁵⁸ These can also be used by influencers.

“Some beauty and health influencers may promote diets that could lead young kids to develop eating disorders or case those who struggle with eating disorders to become worse.” (NICCY Youth Panel)


⁵⁴ See [WP5_online-forum-III_event-report.pdf \(core-evidence-eu.s3.amazonaws.com\)](#) for additional evidence on this.

⁵⁵ [\(PDF\) Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy \(researchgate.net\)](#)

⁵⁶ [ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf](#), p.4

⁵⁷ [Protecting children from harms online - Volume 3: The causes and impacts of online harms to children \(ofcom.org.uk\)](#) p.108.

⁵⁸ [Protecting children from harms online - Volume 3: The causes and impacts of online harms to children \(ofcom.org.uk\)](#) p.58.



It is of note that the NSPCC has recently stated that it expects more contacts from children this summer about body image and eating disorders, causes including spending more time online that might make them feel negatively about the way they look.⁵⁹

“There is a lot, especially suicidal thoughts that I see on TikTok. Like I ran out of lip balm. I think that apps like TikTok, Instagram, YouTube need to have some sort of filter to stop showing this sort of content as you don’t know what’s going through someone’s mind.” (NICCY Youth Panel)

Our Youth Panel questioned how tech companies and Ofcom would be fast enough to keep on top of rapidly changing codes.

“We need to keep up to date with all the bypass methods that are and will be used.” (NICCY Youth Panel)


Access to useful and supportive information and services online was noted as a key right by the Youth Panel with support for recommender systems that would link a young person to available child friendly and accessible support when attempting to access harmful content. Youth Panel members recognised however that sometimes ‘good information’ can share the same space ‘as ‘bad information’ and the potential that some of Ofcom’s proposals might reduce access to ‘good information’. There was also appreciation of Ofcom’s work regarding the ‘evolving capacities’ of young people in relation to risks of harm.

‘Companies’ current business models’ was noted by our Youth Panel as a key impediment to making progress with a high degree of skepticism that Ofcom would be able to effectively hold them to account, particularly in the context of a weak rights framework.

“As long as these large corporations are making huge profits there will be little change. They must prioritise the rights of young people or face the consequences that actually affect them.” (NICCY Youth Panel)

“How will we as young people know if Ofcom as holding companies accountable?” (NICCY Youth Panel)

⁵⁹ https://www.nspcc.org.uk/about-us/news-opinion/2024/Childline-anticipates-summer-spike-in-contacts-from-children-about-body-image-and-eating-disorders/?utm_campaign=20240729_KIS_CASPAR_July29&utm_content=Childline%20expects%20more%20contacts%20from%20children%20this%20summer%20about%20body%20image%20and%20eating%20disorders&utm_medium=email&utm_source=Adestra



NICCY would have wished a stronger focus on ‘safety by design’ principles and more of a focus on upstream design rather than downstream mitigation within this Consultation.

The Safety by Design principles developed by Australian eSafety Commissioner raises user safety as the third pillar in the developmental process for all online and digital technologies, sitting alongside privacy and security. The basic principle is that safety design principles are common across industry. However, the online world was built for speed, not safety. Tech companies should now focus on safety in the same way as, for example, the food, toy, equipment, and automobile industries.⁶⁰ This speaks again to the importance of CRIAs and the prioritisation of children and young people’s rights in wider governance systems. The 5Rights Foundation recommended in their submission to the Online Safety Bill that a ‘safety by design’ framework must carry statutory weight as the primary mechanism by which companies can identify and mitigate the risks posed by their services and fulfil the duty of care. It must be applicable to all products and services likely to be accessed by children.⁶¹ NICCY agrees with this recommendation.

The governance systems of social media platforms should meet the same safeguarding standards as is expected in the offline world. We agree that body image and depressive content be included in the non-designated content; however, we refer to the recommendation from the Scottish Children and Young People’s Commissioner that a thorough CRIA should be undertaken when considering extending the draft Codes to any form of non-designated content and ensure that children actively participate in the proposals.⁶²

A question was raised by a member of our Youth Panel upon reflecting on the 4Cs Framework and the ‘contract’ category:

“How could these Children’s Code limit access to online sales of harmful products?” (NICCY Youth Panel)

In the surveys returned by our Youth Panel, it was clear that the older age group are highly sensitized to the needs of younger children, suggesting that peer relationships might support children to find help when they need it and that equipping older young people with

⁶⁰ [Safety by Design | eSafety Commissioner](#)

⁶¹ [5Rights Foundation](#)

⁶² [DRAFT-OFCOM-Consultation-v2-July-24.pdf \(cypcs.org.uk\)](#)



the knowledge and skills and confidence is a critical piece of this picture. This requires a major investment in media literacy education in schools, reflecting that current provision is piecemeal, inadequate and poorly resourced.

“We need more workshops as young people, but not the ones where you sit in a room for three hours watching a PowerPoint.” (NICCY Youth Panel)

“I think it is important that there are stricter rules on the age that young people and children should be getting access to devices. I know growing up I didn’t get a phone until I was about to start secondary school, and I know that young children seem to be getting them a lot earlier these days. I think younger children are being influenced by social media and more and more people are trying to fit in with others and with trends.” (NICCY Youth Panel)

Recommendation 10: We recommend that Ofcom consider using the 4 Cs Framework when engaging with children and young people in relation to online harms.

Volume 4


It is well documented that most approaches to understanding risks to children do not include a comprehensive review against the full list of child rights. In many cases, assessment methods are risk-based but not rights-based (e.g. not based on child rights frameworks).⁶³

Under the UN Guiding Principles on Business and Human Rights (UNGPs) as well as the Children’s Rights and Business Principles (CRBPs), all companies including those developing, deploying, and using digital technologies have a responsibility to identify and address the adverse human rights impacts with which they are involved – both online and offline. This responsibility is particularly important regarding children’s rights, as the impacts businesses have on children may be severe, long-lasting, and more likely irreversible.⁶⁴

To address this, UNICEF is prototyping a modular CRIA toolkit adapted to the digital environment. The goal of the toolkit is to improve the rigor and consistent adoption of CRIAs in the digital environment and support stakeholders in implementation. The planned content of the Toolkit includes:

⁶³ [Child Rights Impact Assessments in Relation to the Digital Environment.pdf \(unicef.org\)](#) p.6

⁶⁴ Prof. John Ruggie, former Special Representative of the UN Secretary-General for Business and Human Rights and OECD, *What is child vulnerability and how can it be overcome?*, 2019.



1. A Child Rights Overview Deck that provides authoritative overview of child rights, why they are important, and the “business case” for conducting robust CRIAs.

2. A CRIA tool that provides:

- A list of risk and impact statements to assess in relation to child rights in the digital environment with clear signposting of child rights,
- Key considerations delineated by industry actor, type of technology or product feature,
- Key considerations of vulnerability characteristics including individual and environmental factors.


3. Accompanying guidance, including guidance on best practice and baseline expectations for CRIAs in the digital environment; steps to determine appropriate mitigation measures to address salient risks or impacts; advice on incorporating CRIAs into broader human rights assessment or due diligence processes; and best practices for responsible child engagement.⁶⁵

NICCY would welcome a broadening of the risk assessment guidelines by Ofcom to include a comprehensive review of the impact on all children’s rights and we recommend following the UNICEF modular CRIA toolkit.

Implementing effective governance arrangements for prioritising children’s safety goes to the heart of these proposals. We acknowledge the proposed measures for how service providers should approach governance and accountability in relation to the children’s safety duties in the four areas of: governance arrangements; senior accountability and responsibility; internal assurance and compliance functions; and staff policies and practices.

Under the principle of proportionality, we also understand why Ofcom has reduced some of the requirements on smaller lower risk companies due to cost and capacity constraints. However, we are concerned that this might at times undermine responsibilities. For example, Ofcom to require all companies to undertake an annual review of risk management activities in relation to child safety. However, not all companies will be required to ensure that staff involved in the design and operational management of the

⁶⁵ Ibid., p.10



service are trained in the service's approach to compliance with the children's safety duties, including the reporting and complaints duties, sufficiently to give effect to them.⁶⁶

Knowledge and capacity constraints are often cited as obstacles to the integration of children's rights within existing due diligence and compliance efforts. This integration can be hampered by a lack of internal expertise on child rights or understanding of the relevance of child rights for the product, service, or business.⁶⁷ Potentially, the absence of training for smaller companies might undermine the conduct of an effective review which is required by all.

We also note that the 'effective compliance training programme' for children's safety duties makes no mention of children's rights.

Within this volume a distinction is made between 'core inputs' which represent a minimum standard of evidence based on the Online Safety Act and 'enhanced inputs' which have been drawn from industry practice coupled with Ofcom's own research and that of expert third parties.

'Enhanced inputs' seems to speak to the 'safety by design' principles mentioned earlier with companies being asked to consider running tests on new products (this includes any functionality, feature, tool or policy) ahead of launching it on their wider service.⁶⁸ Ofcom suggests that this might include:


“Engaging external organisations representing specific groups to better understand the perspectives of specific users, demographic groups or communities. This will be especially relevant if the service has evidence that certain vulnerable groups will be particularly impacted by content harmful or any aspect of the service's design, including planned design changes which require a risk assessment. This could be particularly helpful for services seeking to consider the risk of content harmful to children presented to children in different age groups.”⁶⁹

⁶⁶ [Protecting children from harms online - Volume 4: Assessing the risks of harms to children online \(ofcom.org.uk\)](https://www.ofcom.gov.uk/consult/condocs/protectingchildren/protectingchildren_volume4.pdf) p.44

⁶⁷ [Child Rights Impact Assessments in Relation to the Digital Environment.pdf \(unicef.org\)](https://www.unicef.org/child-rights-impact-assessments)

⁶⁸ [Protecting children from harms online - Volume 4: Assessing the risks of harms to children online \(ofcom.org.uk\)](https://www.ofcom.gov.uk/consult/condocs/protectingchildren/protectingchildren_volume4.pdf) p.84

⁶⁹ *Ibid.*, p.89



We would like it noted that from NICCY Youth Panel’s perspective, testing new products with children and young people to assess their impact on young people’s safety online should be a ‘core input’.

Recommendation 11: Ofcom to include in their guidance on conducting risk assessments to include a comprehensive review against the full list of child rights in line with the UN Guiding Principles on Business and Human Rights (UNGPs) as well as the Children’s Rights and Business Principles (CRBPs).

Recommendation 12: Ofcom to consider using the UNICEF modular Child Rights Impact Assessment toolkit.

Volume 5

Robust age checks

NICCY recommends that Ofcom widen the criteria for effective age assurance to follow the 5Rights Foundation principles of privacy-preserving, rights-respecting, proportionate to risk and purpose, easy for a child to use, accessible and inclusive, and enhances a child’s experience, rather than merely restricts it, offering a high level of security, transparency, accountability, accepts that a child does not always tell the truth and offers clear routes to challenge and redress. The ultimate purpose of age assurance is to support the protection and flourishing of children and young people.

“Rather than viewing it as simply restricting access, we should be looking at age assurance as a chance to invite children into a digital world that offers them greater privacy, freedom from commercial pressures, content and information in formats and language that they like, protection from misinformation or material that promotes harmful activities (such as suicide, self-harm or disordered eating), alongside supporting digital services in their legal duty not to provide children with age restricted contact and content. Real and effective age assurance can help build the internet that young people deserve.”⁷⁰

The debate around age assurance can often be a perplexing one. In an age where companies are collecting vast amounts of data on users including location, moods, interests, income, sexuality etc. their historical unwillingness to identify children by age

⁷⁰ 5Rights Foundation, p.5



due to 'privacy' and/or 'technical' issues has been puzzling. Effective age assurance will stop companies pretending that children aren't there.

The NICCY Youth Panel offered a number of ideas with regards ways of enhancing the effectiveness of age assurance with the principle that these need to be realistic and not idealistic: the use of ID documents such as passports and birth certificates; creating a digital 'id document' that would only contain information with regards to age; verification from schools; use online age verification systems like Yoti Ltd; products are rated (like the Motion Picture Association) with regards age classifications; develop 'Age Captchas'; age verification cookies; computer software that allows parents to see what content their child has accessed without having to check their child's phone.

"Age verification is way too loose. On Twitter, you can claim any age above 13 without scrutiny and even change your date of birth multiple times. How can children be protected online if companies don't even know they are there." (NICCY Youth Panel)

"I think any user under the age of 16 should automatically be set a 3-hour limit on TikTok or Instagram or any other social media app. If the apps themselves enforce this, it would mean that children can't spend all day sitting on their phones or all day on one app at least." (NICCY Youth Panel)

The Youth Panel agreed with Ofcom's requirement that service providers should take steps to identify any methods children are likely to use to circumvent the age assurance methods implemented and take feasible and proportionate steps to mitigate against the use of these methods of circumvention, in so far as it is possible to do so. They also raised concerns with regards data collection in any age verification processes. No personal data should be collected from young people without their informed consent, which should be based on a clear and highly accessible statement of how their data is to be used; children should be given the option to withdraw consent at any time. Children who cannot give consent should not be asked to provide any personal data online.

Recommender systems

NICCY agrees with the proposed recommender systems measures to be included in the Children's Safety Codes. Several of the NICCY Youth Panel spoke to the business model



driving these recommender systems generating huge advertising revenue for companies. They expressed skepticism that companies will willingly change their recommender systems if this leads to a drop in profits.

NICCY supports the 5Rights Foundation’s recommendations that there should be a requirement on companies to publish information about the algorithms used to prioritise, recommend and moderate content, rank search results and target and profile users. These algorithms are very often the main drivers of harm and the way they are deployed is largely unknown to both users and regulators. Services must make clear the purposes for which algorithms are deployed, the data they are using to feed the algorithms, and the outcomes they produce. Importantly, these outcomes must include both the intended and unintended consequences. Companies must not be permitted to use commercial sensitivity to avoid transparency obligations, and where there are commercial sensitivities, Ofcom must have the power to maintain private oversight.⁷¹

“Try and create a ‘positive’ image/thought with recommender systems.” (NICCY Youth Panel)

“Algorithms should be erasable and reconfigured.” (NICCY Youth Panel)

Effective moderation

NICCY agrees that all user-to-user services should have content moderation systems and processes that ensure swift action is taken against content harmful to children. Search services should also have appropriate moderation systems and, where large search services believe a user to be a child, a ‘safe search’ setting which children should not be able to turn off should filter out the most harmful content.

The NICCY Youth Panel recognised that moderation can be a highly complex process and agreed that priority should be given to the potential severity of content, irrespective of size of audience and how fast it could spread. There is concern however, that content can be removed from one platform, but is available on another almost instantly, posing a problem for online safety and risk of harm.

⁷¹ 5Rights Foundation, p.31



There was also support for Ofcom’s consideration of the different languages spoken by children and young people in the UK, different cultures and the importance of services recruiting moderators with different language and cultural skill sets. There was also an understanding that moderation is a ‘weave’ of human and artificial intelligence and that this mix needs to work for the benefit of children.

“If they are going to use AI for moderation, it would be important to ensure that it is totally reliable. It might be a better idea for actual people to do it who are or who were parents at a stage in their lives, as they might have a better idea of what is appropriate for children.” (NICCY Youth Panel)

“Employ people to monitor their sites that are trained up to remove it and track the perpetrators, along with having more severe penalties for distributing inappropriate content online.” (NICCY Youth Panel)

“Companies could review content before it is posted online, carry out punishments to those posting harmful content, a constant monitoring system which informs individuals of their harmful content so that they are aware that they could be prevented from posting in the future.” (NICCY Youth Panel)

It would therefore be helpful to see an annual moderation report from companies subject to these new Codes.

Strong governance and accountability

We refer to the Children’s Commissioner for England’s response with regards the recommendation to establish a register of the services operating in the UK. This was supported by our Youth Panel. It would seem challenging to hold services to account if there is no complete register of these services.

Child-friendly justice processes for children and young people to act on a breach of the duty to care is a critical part of these Children’s Codes. The NICCY Youth Panel wished to see greater details on how this might work including Ofcom’s remit to take individual complaints from minors.



The Council of Europe’s guidelines to respect, protect and fulfil the rights of the child in the digital environment state that Member States should fulfill a child’s right to an effective remedy when their rights have been infringed in the digital environment. This entails providing accessible, affordable and child-friendly routes through which children, parents and legal representatives may submit complaints and seek remedies.⁷²

More choice and support for children

The NICCY Youth Panel had no disagreement with Ofcom’s requirements regarding the improvements providers need to make to their reporting systems. Whilst Ofcom has not decided on whether it might be practical to require companies to report back to children on the outcome of their complaints, our Youth Panel felt that this would be critical to build trust in the system.

Different reasons were offered as to why young people might or might not report and what might help.

“I’d say a lot of young people who accidentally see harmful content don’t report it because they want to learn more about it or are interested by it.” (NICCY Youth Panel)


“I do report harmful content because I feel like it can really affect young people’s mental health and have real negative effect on them.” (NICCY Youth Panel)

“Maybe young people could get some sort of incentive for reporting; they shouldn’t need to have an incentive but that always seems to work with young people.” (NICCY Youth Panel)

“Reporting services are not always easy to access and people have to go searching for it in many cases. Young people may not know how to report harmful content and therefore an introduction could be given at the initial download of the platform.” (NICCY Youth Panel)

“Being reminded regularly (for example at school) to report harmful content so that we can feel more comfortable and less hesitant to report something.” (NICCY Youth Panel)

⁷² See Guidelines to respect, protect and fulfil the rights of the child in the digital environment [16808d881a \(coe.int\)](https://www.coe.int/t/e/childrights/childrights/childrights_en.asp)



“I would report bad content if it’s misinformation or someone being taken advantage of or a young person in a bad situation. If it’s just a young person creating a silly video that’s safe, then no, would not report it.” (NICCY Youth Panel)

“Don’t let young people on social media. It’s toxic! Seriously if life didn’t evolve around these devices, I wouldn’t be on it. Most days I wish I wasn’t.” (NICCY Youth Panel)

“If you’re on a site that is explicit there’s no point reporting; you just have to move on.” (NICCY Youth Panel)

“Should have children’s phones so that kids are exposed to explicit content.” (NICCY Youth Panel)

“I think there needs to be more awareness about how crucial reporting harmful content is. Maybe adverts that interrupt scrolling to stress the importance of reporting something if you see it.” (NICCY Youth Panel)

“There is fear surrounding harmful content, such as getting into trouble with their family and feeling guilty and responsible. A safe reporting form needs to be given and encouraging young people. An introduction when downloading an app to reporting would also be beneficial.” (NICCY Youth Panel)

“To be honest I think there shouldn’t be a minimum age for smart phones as I live in the countryside and rely on my phone when I’m out without my parents. It’s on the parents that they should be the ones keeping the rules and boundaries. For example, not having my phone past a certain time and so on.” (NICCY Youth Panel)

“Get rewards and free credits for reporting. E.g. report three harmful posts and you get 1-month free premium.” (NICCY Youth Panel)

There were different suggestions for making terms of reference accessible and clear. There was broad support for the principle that an easy-read document would be beneficial for children and adult users. In general, more information and education were seen as key.

“I think that there should be more awareness lessons and skills and new clubs. I know that there’s the Internet Safety Week and opportunities for different organisations to talk more about internet safety, but I think it should be like a regular thing every week because young people just forget or don’t listen. I think that young people’s parents should also be talking about it.” (NICCY Youth Panel)



“Education in school, and a compulsory slide show or information that must be read when setting up a first phone (unless data is carried over from an old phone when setting up, so it’s clear that you have previously owned one). And this must be read so you can’t scroll, and press agree; there should be time sensor set so that it must be scrolled through slowly so that it’s actually read before ‘agreeing’ to any policies and agreeing to have a phone while learning safety regulations.” (NICCY Youth Panel)

There was strong support for Ofcom’s proposal that providers should signpost children to support at key points in the user journey when they encounter suicide, self-harm, eating disorder or bullying content and they welcome Ofcom’s commitment to exploring how this measure could be extended to other kinds of harmful content.

The importance of a strong vibrant community and voluntary support infrastructure ensuring that children and young people’s digital and online rights are being safeguarded cannot be underestimated, as well as providing more activities in the offline world.

“The only support service that I am aware of is the Log Off Movement which is a charity in America and has been adopted worldwide. I help them by creating content and reviewing their resources, and I think it’s important that young people are with different charities that can support them. Social media is such a big thing that affects young people physically and mentally.” (NICCY Youth Panel)

“Invest more in youth services including making transport cheaper so that young people can go on day trips.” (NICCY Youth Panel)

“More parents should be encouraged to take responsibility for how much time their child spends on their phone. Parents can easily set a time limit on a child’s phone for how much time they spend on it a day. Children should be encouraged more to do other activities rather than spending time on their phone. This means stopping the cuts to our youth clubs and youth services.” (NICCY Youth Panel)

“Don’t listen to uneducated authority figures as they often don’t know what they are talking about and can inadvertently spread harmful information.” (NICCY Youth Panel)

Recommendation 13: Ofcom to establish and update a register of services operating in the UK.



Recommendation 14: Ofcom to develop child-friendly justice processes for children and young people to act on a breach of the duty to care.

8. Conclusions

“I never feel safe online.” (NICCY Youth Panel)

Out of all the quotes and reflections from our Youth Panel, this was one of the most poignant. We know that only 44% of young people trust social media companies to prioritise young people’s safety online as technology changes.⁷³ Against this backdrop of relatively low trust, young people overwhelmingly want more of a voice, with 80% saying that young people should be listened to more about changes in technology, such as how it can remain safe.⁷⁴

While awareness of the Online Safety Act is relatively low among both young people and parents and carers, once explained, support for its intention is very high.⁷⁵ NICCY considers that Ofcom have missed an opportunity to build the awareness and the trust needed in this consultation by not centering children’s rights, as outlined in the UNCRC and GC25, at the heart of these Children’s Codes. In addition, whilst we understand the need for the technical and legal terms and analysis, the document’s length and complexity will not build confidence and encourage the participation of children and young people, parents and carers and wider civil society.

The long journey of the Online Safety Act and the projected timeframes with regards the publication of these Children’s Codes and other elements of the Act does not create confidence that our regulatory system will be able to match the nimbleness and speed in our digital world. Young people need to feel safe online today.

There is uncertainty about the future shape of the online world and the development of artificial intelligence (AI) and there is a non-trivial possibility that the actions that tech companies will take now will cause irreversible harm. In this context, the burden of proof should be on the companies proving safety, not the other way round. Currently, only when there is irrefutable evidence of harm does the law eventually come in to regulate. When we are talking about technology that is radically more powerful, and radically faster moving and scaling up than government – the potential harm that is caused by, for example, AI requires a precautionary principle. This says if there is significant uncertainty and radical

⁷³‘A summary report by the UK Safer Internet Centre for Safer Internet Day 2024’ [UKSIC-2024-Executive-Summary-Report.pdf \(d1xsi6mgo67kia.cloudfront.net\)](https://www.uk-saic.org/2024/01/16/summary-report/)

⁷⁴ Ibid.

⁷⁵ Ibid.



consequences in that space then the burden of proof is on proving safety and that needs evidenced before being able to move forward. This will demand a very different approach to regulation and tech design. It is worthwhile noting that the current and potential harm children and young people face in the digital world is not limited to immediate harms but also to the wider harms with regards to the environmental and climatic consequences as companies continue to externalise the costs.

One of the roles of regulator is to lift the ‘hood’ and ask the right questions. Companies’ business model is and will be to ‘outwit’ these questions and to minimise any information that might impact on this business model. The absence of any details with regards the regulatory review of the Act and how children and young people will know whether these Children’s Codes have led to, for example, girls and women facing less gendered harm and abuse, have protected children from harmful content including pornography, have made it easier to report with young people seeing the impact of their reporting, is another missed opportunity.

NICCY’s Youth Panel has committed to playing their part in creating a standing agenda item at their quarterly meetings to monitor the impact of the Act and these Codes, linking into NI’s Online Safety Strategy. Only through the participation of children and young people will children and young people get the online world they want and the online world they deserve. NICCY welcomes this Consultation and the opportunity to respond to it.

