

# Submission to Coimisiún na Meán on Developing Ireland's First Binding Online Safety Code for Video-Sharing Platform Services

September 2023



Founded in 1995, the Children’s Rights Alliance unites over 140 members working together to make Ireland one of the best places in the world to be a child. We change the lives of all children in Ireland by making sure that their rights are respected and protected in our laws, policies and services.

Accompaniment Support Service for Children (A.S.S.C.)  
Alcohol Action Ireland  
Amnesty International Ireland  
An Cosán  
Anew  
Anne Sullivan Foundation  
Aoibhneas  
Archways  
AsIAm  
Association of Occupational Therapists of Ireland (AOTI)  
Association of Secondary Teachers Ireland (ASTI)  
ATD Fourth World – Ireland Ltd  
Atheist Ireland  
Barnardos  
Barretstown Camp  
Bedford Row Family Project  
BeLonG To Youth Services  
Bodywhys  
Catholic Guides of Ireland  
Child Law Project  
Childhood Development Initiative  
Children in Hospital Ireland  
Children’s Books Ireland  
Children’s Grief Centre  
Clarecare  
COPE Galway  
Cork Life Centre  
Cork Migrant Centre  
Crann Centre  
Crosscare  
CyberSafeKids  
Cycle Against Suicide  
Dalkey School Project National School  
Daughters of Charity Child and Family Service  
Dental Health Foundation of Ireland  
Department of Occupational Science and Occupational Therapy, UCC  
Disability Federation of Ireland  
Doras  
Down Syndrome Ireland  
Dublin Rape Crisis Centre  
Dyslexia Association of Ireland  
Dyspraxia/DCD Ireland  
Early Childhood Ireland  
Early Learning Initiative (National College of Ireland)  
Educate Together  
EPIC  
Equality for Children  
Extern Ireland  
FamiliBase  
Féach  
Focus Ireland  
Foróige  
Gaeloideachas  
Galway Traveller Movement  
Good Shepherd Cork  
Grow It Yourself  
Helium Arts  
Immigrant Council of Ireland  
Inclusion Ireland  
Institute of Guidance Counsellors  
Irish Aftercare Network  
Irish Association for Infant Mental Health  
Irish Association of Social Workers  
Irish Congress of Trade Unions (ICTU)  
Irish Council for Civil Liberties (ICCL)  
Irish Foster Care Association  
Irish Girl Guides  
Irish Heart Foundation  
Irish National Teachers Organisation (INTO)  
Irish Penal Reform Trust  
Irish Primary Principals’ Network  
Irish Refugee Council  
Irish Second Level Students’ Union (ISSU)  
Irish Society for the Prevention of Cruelty to Children  
Irish Traveller Movement  
Irish Youth Foundation  
iScoil  
Jigsaw  
Katharine Howard Foundation  
Kerry Diocesan Youth Service (KDYS)  
Kids’ Own Publishing Partnership  
Kinship Care  
Leap Ireland  
Let’s Grow Together! Infant and Childhood Partnerships CLG.  
LGBT Ireland  
Meath Women’s Refuge & Support Services  
Mecpaths  
Mental Health Reform  
Mercy Law Resource Centre  
Migrant Rights Centre Ireland  
Mothers’ Union  
Museum of Childhood Ireland  
Music Generation  
My Mind  
My Project Minding You  
National Childhood Network  
National Council for the Blind of Ireland  
National Forum of Family Resource Centres  
National Parents Council Post Primary  
National Parents Council Primary  
National Youth Council of Ireland  
New Directions  
Novas  
One Family  
One in Four  
Parents Plus  
Pavee Point  
Peter McVerry Trust  
Prevention and Early Intervention Network  
Psychological Society of Ireland  
Rainbow Club Cork  
Rainbows Ireland  
Rape Crisis Network Ireland (RCNI)  
Realt Beag/Ballyfermot Star  
Respond Housing  
SAFE Ireland  
Saoirse Housing Association  
SAOL Beag Children’s Centre  
School of Education UCD  
Scouting Ireland  
Sexual Violence Centre Cork  
Simon Communities of Ireland  
SIPTU  
Social Care Ireland  
Society of St. Vincent de Paul  
SPHE Network  
SpunOut.ie  
St. Nicholas Montessori College  
St. Nicholas Montessori Teachers’ Association  
St. Patrick’s Mental Health Services  
TASC  
Teachers’ Union of Ireland  
Terenure College Rugby Football Club  
The Ark, A Cultural Centre for Children  
The Irish Red Cross  
The Jack and Jill Children’s Foundation  
The UNESCO Child and Family Research Centre, NUI Galway  
The Wheel  
Transgender Equality Network Ireland  
Traveller Visibility Group Ltd  
Treoir  
UNICEF Ireland  
Variety – the Children’s Charity of Ireland  
Women’s Aid  
Young Ballymun  
Young Social Innovators  
Youth Advocate Programme Ireland (YAP)  
Youth Work Ireland

## Children’s Rights Alliance

7 Red Cow Lane, Smithfield, Dublin 7, Ireland

Ph: +353 1 662 9400

Email: [info@childrensrights.ie](mailto:info@childrensrights.ie)

[www.childrensrights.ie](http://www.childrensrights.ie)

© 2023 Children’s Rights Alliance – Republic of Ireland Limited

The Children’s Rights Alliance is a registered charity – CHY No. 11541

## Introduction

---

**The Children’s Rights Alliance unites over 140 organisations working together to make Ireland one of the best places in the world to be a child. We change the lives of all children in Ireland by making sure that their rights are respected and protected in our laws, policies and services. We identify problems for children. We develop solutions. We educate and provide information and legal advice on children's rights.**

**The Children’s Rights Alliance is also a member and National Partner of Eurochild, the largest network of organisations and individuals working with and for children in Europe. Eurochild works closely with the European Union, as protecting children’s rights is among the EU’s aims and values.**

The Children’s Rights Alliance welcomes the opportunity to make a written submission to Coimisiún na Meán on developing Ireland’s first binding Online Safety Code for video-sharing platform services.

Children make up one third of global online users.<sup>1</sup> Results from a National Survey of Children, their Parents and Adults regarding Online Safety conducted between December 2019 and October 2020, found that 62 per cent of children and young people in Ireland, aged nine to 17 years use social media.<sup>2</sup> This rises to 90 per cent of 15 to 17 year olds.<sup>3</sup> While the online world brings unparalleled opportunity to children to learn, create, connect and socialise, it also brings risk, including the loss of personal data, exposure to harmful content, cyberbullying, negative impacts on health and well-being, online grooming and extortion. In 2021, CyberSafeKids reported that a quarter of all children they worked with<sup>4</sup> surveyed have seen or experienced something online in the last year that bothered them, with almost one third of those children having kept it to themselves rather than report it to their parents or someone else.<sup>5</sup>

The UN Committee on the Rights of the Child have acknowledged the increasing importance of the digital environment in that it ‘affords new opportunities for the realization of children’s rights, but also poses the risks of their violation or abuse.’<sup>6</sup>

While undoubtedly, the internet has significant positive impacts both for children and wider society, for too long legislation and policy have not kept pace with the evolution of the online world. This has left children and young people at risk and unprepared to appropriately navigate online platforms. The introduction of the Online Safety and Media Regulation Act 2022 and the Digital Services Act will pave the way for a new era of online regulation. Central to this is the introduction of the Online Safety Codes. We welcome to opportunity to take part in the consultation process and look forward to continued engagement to make the online world safer for children and young people.

---

<sup>1</sup> Unicef, *Children in the Digital World* (UNICEF 2017).

<sup>2</sup> National Advisory Council for Online Safety, *Report of a National Survey of Children, their Parents and Adults regarding Online Safety 2021* (2021) 8.

<sup>3</sup> *ibid.*

<sup>4</sup> CybersafeKids gathered data from 4,714 children over the 2021/22 academic year CyberSafeKids, *Annual Report 2021* (2022) 5.

<sup>5</sup> CyberSafeKids, *Annual Report 2021* (2022) 3.

<sup>6</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, *CRC/C/GC/25*, para 3.

## Question 1: What do you think our main priorities and objectives should be in the first binding Online Safety Code for VSPS? What are the main online harms you would like to see it address and why?

### **Main priorities and objectives**

The UN Committee on the Rights of the Child are clear that ‘the rights of every child must be respected, protected and fulfilled in the digital environment.’<sup>7</sup> This should be one of the main objectives of the first binding Online Safety Code.

The UN Committee on the Rights of the Child provides that States should ‘take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse...’<sup>8</sup> Further it requires States to ‘ensure that relevant legislation provides adequate protection of children in relation to media and ICT’.<sup>9</sup> This should be one of the main priorities and objectives of the Code.

The Committee has also recommend 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.’<sup>10</sup> The Council of Europe (COE) *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment* provide that ‘in all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration’ and further recommend that States should strike a balance between the child’s right to protection and their other rights to freedom of expression, participation and access to information.<sup>11</sup> The COE also acknowledges the differing levels of maturity and understanding of children at different ages and recommends that States recognise the evolving capacities of children which can mean that the ‘policies adopted to fulfil the rights of adolescents may differ significantly from those adopted for younger children’.<sup>12</sup>

The Committee on the Rights of the Child in 2013 issued a General Comment<sup>13</sup> which has clarified the meaning of this principle in 2013 and stated that it has a three-fold meaning. The best interests principle is:

(a) A substantive right: The right of the child to have his or her best interests assessed and taken as a primary consideration when different interests are being considered in order to reach a decision on the issue at stake, and the guarantee that this right will be implemented whenever a decision is to be made concerning a child, a group of identified or unidentified children or

---

<sup>7</sup> *ibid* para 4.

<sup>8</sup> UN Convention on the Rights of the Child, A/ RES/44/25 (20 November 1989) Arts 19.1

<sup>9</sup> UN Committee on the Rights of the Child, General Comment no 13(2011) on the right of the child to freedom from all forms of violence, CRC/C/GC/13 para41(g).

<sup>10</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25 para 12.

<sup>11</sup> *ibid*, 12.

<sup>12</sup> Council of Europe, ‘*Recommendation 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*’ (COE 2018) <<https://bit.ly/2Xp9hpE>> accessed 26 February 2021, 12.

<sup>13</sup> UN Committee on the Rights of the Child (2013) *General Comment No. 14: The right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*, CRC/C/GC/14.

children in general. Article 3, paragraph 1, creates an intrinsic obligation for States, is directly applicable (self-executing) and can be invoked before a court.

(b) A fundamental, interpretative legal principle: If a legal provision is open to more than one interpretation, the interpretation which most effectively serves the child's best interests should be chosen. The rights enshrined in the Convention and its Optional Protocols provide the framework for interpretation.

(c) A rule of procedure: Whenever a decision is to be made that will affect a specific child, an identified group of children or children in general, the decision-making process must include an evaluation of the possible impact (positive or negative) of the decision on the child or children concerned. Assessing and determining the best interests of the child require procedural guarantees. Furthermore, the justification of a decision must show that the right has been explicitly taken into account. In this regard, States parties shall explain how the right has been respected in the decision, that is, what has been considered to be in the child's best interests; what criteria it is based on; and how the child's interests have been weighed against other considerations, be they broad issues of policy or individual cases.

The Alliance believes that one of the main priorities should be ensuring that the best interests of the child is a primary consideration in the Code. Alongside this the Code needs to acknowledge the 'evolving capacities of the child as an enabling principle that addresses the process of their gradual acquisition of competencies, understanding and agency' as 'risks and opportunities associated with children's engagement in the digital environment change depending on their age and stage of development.'<sup>14</sup>

Many of the digital services children and young people use are not designed to protect their rights or meet their needs.<sup>15</sup> Research from the 5Rights Foundation found that 'pathways designed into digital services and products are putting children at risk' with designers tasked with 'optimising products and services for three primary purposes, all geared towards revenue generation.'<sup>16</sup> The Online Safety Code presents a huge opportunity to embed the principle of safety by design into the Irish regulatory framework. It is important that this principle is not incorporated only to services specifically targeted to children and young people but to all the digital services children and young people are likely to actually access.<sup>17</sup>

## Recommendations

- Ensure that the protection and fulfilment of children's rights online is a primary objective of the Code. In particular ensure that:
  - the right of the child to protection from abuse and exploitation online is embedded as a key principle.

---

<sup>14</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 19

<sup>15</sup> 5Rights Foundation, 'Design of Service' <<https://5rightsfoundation.com/our-work/design-of-service/>> accessed 4 September 2023.

<sup>16</sup> 5Rights Foundation, September 2021 Pathways: A Summary Key findings and recommendations from Pathways: How digital design puts Children at Risk (2021) 7.

<sup>17</sup> 5Rights Foundation, 'Design of Service' <<https://5rightsfoundation.com/our-work/design-of-service/>> accessed 4 September 2023.

- the best interests of every child is a primary consideration in all actions affecting them.
- Embed safety by design into the Online Safety Code as one of the main priorities and objectives.

### **Main Harms**

The harms listed in the ‘Call for Inputs’ need to all form part of the online harms the code seeks to address.

The four areas set out in Article 28b of the Audio- Visual Media Services Regulation need to be addressed by the Online Safety Code:

1. Content that might impair the physical, mental or moral development of minors. This includes content that may be inappropriate for children, such as pornography.
2. Content that incites violence or hatred against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the European Charter of Fundamental Rights. These grounds include sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.
3. Content the dissemination of which constitutes a criminal offence under EU law.
4. Certain commercial communications that would not be permitted on broadcast or video-on-demand services. Commercial communications include advertising, sponsorship and product placement.

The categories of harm set out in the Broadcasting Act 2009 Act as amended by the Online Safety and Media Regulation Act 2022 also should be addressed by the online safety code:

- a. Harmful online content relating to 42 criminal offences under Irish law listed in Schedule 3 of the 2009 Act as amended
- b. Online content by which a person bullies or humiliates another person;
- c. Online content by which a person promotes or encourages behaviour that characterises a feeding or eating disorder;
- d. Online content by which a person promotes or encourages self-harm or suicide;
- e. Online content by which a person makes available knowledge of methods of self-harm or suicide;

Consultations with children and young people have shown that they are most disturbed by violent content online, it is key that the Code addresses this.<sup>18</sup> Consideration should also be given to addressing Harmful Commercial Communications, particularly marketing of high fat, sugar and salt foods and breastmilk substitutes as there are heightened risks of, and harms associated with, commercial exploitation and negative impact on development and health that can occur as a result of marketing practices of these foods.<sup>19</sup> Alcohol is one of the most heavily marketed products and as

<sup>18</sup> EU Kids Online ‘EU Kids Online 2020: Survey results from 19 countries’ < <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020>> accessed 4 September 2023, 142,149,151.

<sup>19</sup> Irish Heart Foundation, Submission to Coimisiún na Meán Call For Inputs on Developing First Online Safety Code 2023.

such it is important that the new Online Safety Code protect children and the general public from the harmful commercial practices.<sup>20</sup>

Online racism and hate speech against minority groups such as Traveller and Roma, Lesbian, Gay, Bisexual and Transgender (LGBT) young people, black and ethnic minorities people should form part of the harms that the Online Safety Code seeks to address. The new Online Safety code should seek to align with the Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 that is currently going through the Oireachtas. This legislation will contain a list of protected characteristics such as race, colour, nationality, religion, national or ethnic origin, descent, gender, sex characteristics, sexual orientation, disability, and also specifically recognises Travellers as an ethnic group. It states – “references to “national or ethnic origin” include references to membership of the Traveller community (within the meaning of section 2(1) of the Equal Status Act 2000),”

### Recommendations

- The harms listed in the ‘Call for Inputs’ need to all form part of the online harms the code seeks to address.
- Ensure that the Code addresses children’s exposure to violent content online.
- Consideration should also be given to addressing Harmful Commercial Communications, particularly marketing of high fat, sugar and salt foods and breastmilk substitutes and alcohol.

---

<sup>20</sup> Alcohol Action Ireland, Submission to Coimisiún na Meán Call For Inputs on Developing First Online Safety Code 2023.

## Question 2: What types of online harms do you think should attract the most stringent risk mitigation measures by VSPS? How could we evaluate the impact of different types of harms e.g. severity, speed at which harm may be caused? Is there a way of classifying harmful content that you consider it would be useful for us to use?

### *Types of Harm*

There needs to be stringent risk measures imposed on illegal and harmful content for children and young people. In particular there is a need to guarantee that the Code ensures that illegal material such as child sexual abuse materials, intimate images and material that incites hatred can be robustly and swiftly removed. Consultations with children and young people have shown that they are most disturbed by violent content online, it is key that the Code addresses this.<sup>21</sup>

The UN Convention on the Rights of the Child (UNCRC) guarantees all children the right to be protected from abuse, neglect and sexual exploitation.<sup>22</sup> There is growing concern that online grooming, as well as the sharing of child exploitation material, increased online during Covid-19.<sup>23</sup> Irish teenagers are the fourth highest users in the EU for sexting.<sup>24</sup> A recent Report from the Children’s Commissioner for England found that pornography consumption is widespread among children with 13 years old being the average age of first exposure.<sup>25</sup> A significant minority of children are first exposed to pornography at a very young age, 10 per cent of the over 1,000 young people surveyed had seen it by age nine, 27 per cent had seen it by age 11 and 50 per cent had seen it by 13.<sup>26</sup> The Children’s Commissioner Report also found that children ‘often stumble accidentally across pornography online’<sup>27</sup> and Twitter is the platform where the greatest number of children had seen pornography.<sup>28</sup> The majority, 79 per cent of 18-21 year olds surveyed had seen content involving sexual violence before turning 18, and 47 per cent of all those surveyed stated that ‘girls expect sex to involve physical aggression such as airway restriction or slapping.’<sup>29</sup> The Children’s Commissioner is conscious in the report that age verification will not be a ‘silver bullet’ for regulating online pornography as some teenagers, particularly older teenagers may continue to access online pornography.<sup>30</sup> The Code needs to take measures to address children’s access to pornography and the advertising of prostitution.

The production and distribution of child sexual abuse and exploitation materials – whether in print, online, or livestreamed – represent a fundamental violation of children’s rights and a breach of the UNCRC.<sup>31</sup> These images effectively represent a digital crime scene, and people accessing these images directly contribute to the exploitation of child victims by creating demand and perpetuating the child’s trauma. This abuse is ongoing until the image is removed. In 2021, the Internet Watch

---

<sup>21</sup> EU Kids Online ‘EU Kids Online 2020: Survey results from 19 countries’ <<https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020>> accessed 4 September 2023, 142,149,151.

<sup>22</sup> UN Convention on the Rights of the Child, A/ RES/44/25 (20 November 1989) Arts 19 and 34.

<sup>23</sup> Interpol, ‘Child Sexual Exploitation and Abuse threats and trends: COVID-19 Impact’ <<https://bit.ly/34unFDS>> accessed 1 February 2022.

<sup>24</sup> Dublin City University, ‘Irish Teens the Fourth Highest in the EU for Sexting’ <<https://bit.ly/3qTC2HK>> accessed 6 January 2022. See also: Raymond Arthur, ‘Policing Youth Sexting in Ireland’ (2019) 22(3) Irish Journal of Family Law 66.

<sup>25</sup> Children’s Commissioner for England, ‘A lot of it is actually just abuse’ Young people and pornography’ January 2023, 6-8.

<sup>26</sup> *ibid.*

<sup>27</sup> *ibid.*

<sup>28</sup> *ibid.*

<sup>29</sup> *ibid.*

<sup>30</sup> *ibid.*

<sup>31</sup> UN Convention on the Rights of the Child, A/ RES/44/25 (20 November 1989) Arts 19 and 34.

Foundation received a 64 per cent increase in reports, of which 252,194 reports were confirmed as containing child sexual abuse and exploitation material.<sup>32</sup> Similarly, Hotline.ie, the Irish national reporting centre for illegal online content, has experienced a dramatic increase in demand for its services – in 2021 it saw 29,794 reports, which was as many as the previous three years combined.<sup>33</sup> Despite this, Irish cases involving the distribution of child abuse material are taking up to 10 years for the State to complete, with the problem accelerating in recent years, as technological and data issues impede prosecutions.<sup>34</sup> There is a need to ensure that the Code provide for mechanisms for material to be removed swiftly.

### ***Classifying Harmful Content***

The Council of Europe has recommended that ‘states should co-operate with a view to promoting standardisation of content classification and advisory labels among countries and across stakeholder groups to define what is appropriate and what is inappropriate for children.’<sup>35</sup> There are a number of frameworks that could be considered.

#### *CO:RE 4Cs classification*

A key tool to identify risk and classification of harm is the 4Cs framework. The CO:RE 4Cs classification recognises that online risks arise when a child:

- Engages with and/or is exposed to potentially harmful content
- Experiences and/or is targeted by potentially harmful contact
- Witnesses, participates in and/or is a victim of potentially harmful conduct
- Is party to and/or exploited by a potentially harmful contract<sup>36</sup>

The 4Cs classification ‘distinguishes between aggressive, sexual and value risks’ along with recognising important cross-cutting risks such as children’s right to privacy and fair treatment.<sup>37</sup>

---

<sup>32</sup> The Internet Watch Foundation, ‘IWF Annual Report 2021 – Face the Facts’ < <https://www.iwf.org.uk/about-us/who-we-are/annual-report-2021/> > accessed 22 November 2022.

<sup>33</sup> Hotline.ie, *2021 Annual Report (2022)* 7-8.

<sup>34</sup> Conor Gallagher, ‘Backlogs a dangerous flaw in child porn and abuse inquiries Resource and Data leave perpetrator at large – and child vulnerable to further abuse’ *The Irish Times*, 7 January 2020.

<sup>35</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 29, para 121.

<sup>36</sup> CORE, ‘4 Cs of online risk: Short report & blog on updating the typology of online risks to include content, contact, conduct, contract risk’ <<https://core-evidence.eu/posts/4-cs-of-online-risk>> accessed 28 August 2023.

<sup>37</sup> *ibid.*

 CORE	<b>Content</b> Child as recipient	<b>Contact</b> Child as participant	<b>Conduct</b> Child as actor	<b>Contract</b> Child as consumer
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
<b>Sexual</b>	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
<b>Values</b>	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
<b>Cross-cutting</b>	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

38

### *Australian Classification Scheme*

A classification scheme is in place in Australia where the Australian Online Safety Act (2021) defines content as either ‘class 1 material’ or ‘class 2 material’.<sup>39</sup> Class 1 material and class 2 material are defined by reference to Australia’s National Classification Scheme, which is also used for classification of films, computer games and other publications.

Class 1 material includes material that:

- ‘depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence.’

Class 2 material is material that is, or would likely be, classified as either:

- ‘X18+ (or, in the case of publications, category 2 restricted), or
- R18+ (or, in the case of publications, category 1 restricted) under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old.’

The eSafety Commissioner works with online service providers to ensure access to Class 2 material, which is considered unsuitable for children and young people under 18, is restricted.

<sup>38</sup> CORE, ‘4 Cs of online risk: Short report & blog on updating the typology of online risks to include content, contact, conduct, contract risk’ <<https://core-evidence.eu/posts/4-cs-of-online-risk>> accessed 28 August 2023.

<sup>39</sup> Online Safety Act 2021 s106 and s107.

## UK Classification Scheme

The UK Online Safety Bill currently going through the houses of parliament classifies online content that is harmful to children into two distinct categories – primary priority content, and priority content.<sup>40</sup> Primary priority content that is harmful to children includes pornographic content, content which encourages, promotes or provides instructions for an act of deliberate self-injury, suicide, or eating disorders or behaviour associated with eating disorders.<sup>41</sup> Content also falls within the primary priority category if it consists only of text or text accompanied by identifying content which consist only of text, other identifying content which is not itself pornographic, a GIF which is not itself pornographic, an emoji or other symbol, or any combination of these.<sup>42</sup> Priority content that is harmful to children includes content which is abusive and targets race, religion, sex, sexual orientation, disability, or gender reassignment, content which incites hatred against people of any of the above named groups, bullying content, content depicting real or realistic serious violence against a person (not limited to a real person) or animal, or serious injury of a person (not limited to a real person) or animal in graphic detail, as well as serious violence or injury against a fictional creature in graphic detail.<sup>43</sup> Also falling within the priority content category is content which encourages, promotes or provides instructions for a challenge or stunt highly likely to result in serious injury to the person who does it or someone else, content encouraging a person to self-administer a physically harmful substance or a substance in a quantity that is physically harmful.<sup>44</sup>

Under section 63 of the UK Online Safety Bill the Office of Communications (OFCOM) must review the incidence on regulated user-to-user services, search services and combined services of content that is harmful to children, and the severity of harm that children in the UK suffer or may suffer as a result of such content.<sup>45</sup> Arising from this OFCOM must publish a report every three years at least on the outcome of the review and make recommendations as to whether changes are required for sections 61 and 62 covering primary priority content and priority content.<sup>46</sup>

## Recommendations

- Provide for mechanisms in the Code for child sexual abuse material to be removed swiftly.
- Take measures in the Code to address children’s access to pornography and the advertising of prostitution.
- Ensure that the Code provides that illegal material such as child sexual abuse materials, intimate images and material that incites hatred can be robustly and swiftly removed.
- Ensure that the Code addresses violent content online.

---

<sup>40</sup> UK Online Safety Bill, section 60(1).

<sup>41</sup> *ibid* section 61(2) – (5).

<sup>42</sup> *ibid* section 61(6).

<sup>43</sup> *ibid* section 62(1) – (7).

<sup>44</sup> *ibid* section 62(8) – (10).

<sup>45</sup> *ibid* section 63.

<sup>46</sup> *ibid*.

### Question 3: Do you have reports, academic studies or other relevant independent research that would support your views? If you do, please share them with us with links to relevant reports, studies or research.

- 5Rights Foundation, But how do they know it is a child? Age Assurance in the Digital World
- 5Rights Foundation, Making Child Online Safety a Reality: Global Toolkit
- 5Rights Foundation, Pathways: A Summary Key findings and recommendations from Pathways: How digital design puts children at risk
- 5Rights Foundation, Tick to Agree Age appropriate presentation of published terms September 2021
- Child Rights Impact Assessment A tool to realise children's rights in the digital environment March 2021
- Council of Europe Handbook for policy makers on the rights of the child in the digital environment
- Council of Europe published its Recommendation, *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment*
- Livingstone, Sonia (2016) A framework for researching Global Kids Online: understanding children's well-being and rights in the digital age. Global Kids Online. London School of Economics and Political Science, London, UK.
- Livingstone, Sonia and Pothong, Kruakae (2023) Child rights by design: guidance for innovators of digital products and services used by children. . Digital Futures Commission, 5Rights Foundation, London, UK.
- Livingstone, Sonia and Third, Amanda (2017) Children and young people's rights in the digital age: an emerging agenda. New Media & Society.
- Mukherjee, Sudeshna, Pothong, Kruakae and Livingstone, Sonia (2021) Child rights impact assessment: a tool to realise children's rights in the digital environment, Digital Futures Commission, 5Rights Foundation, London, UK.
- UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25
- World Health Organisation, Policies to protect children from the harmful impact of food marketing: WHO guidelines (WHO 2013)
- Beating Eating Disorders UK, [Online advertising and eating disorders](#)
- Sonia Livingstone and Mariya Stoilova, ['The impact of digital experiences on adolescents with mental health vulnerabilities'](#) (2021)

## Question 4: What approach do you think we should take to the level of detail in the Code? What role could non-binding guidance play in supplementing the Code?

The Online Safety Code should take the form of a detailed prescriptive Code. As noted in the ‘Call for Submissions’ this would allow the Code to ‘specify details in the measures we expect VSPS providers to take to address online harms.’

The UN Committee on the Rights of the Child in its General Comment no.25 on children’s rights in relation to the digital environment state that States should require the business sector to undertake children’s rights due diligence and child rights impact assessments and disclose them to the public with consideration of the ‘severe impacts of the digital environment on children.’<sup>47</sup> The UN Committee also state that States should require all businesses that affect children’s rights in relation to the digital environment to implement regulatory codes and frameworks to adhere to the highest levels of privacy and safety standards.<sup>48</sup> They also recommend that States encourage them to take accountability and measures to innovate in the best interests of the child.<sup>49</sup>

A comprehensive legal and regulatory framework in this space should encompass both protective and preventive measures, prohibiting all forms of violence, exploitation and abuse; include child-friendly mechanisms for consultation and participation; provide support measures for parents and carers; and ensure effective remedies.<sup>50</sup> Children’s digital media choices and data control possibilities are shaped by the design and functionalities of communication spaces, control of which rests neither with them, their parents or indeed national regulators.<sup>51</sup>

Legal frameworks should cover the full range of unlawful acts which can be committed online,<sup>52</sup> and there should be a co-regulatory framework that defines the roles and responsibilities of all organisations operating in the digital space.<sup>53</sup> Minimum standards that focus on child safety and the full realisation of children’s rights should be established that cover all actors in the chain.<sup>54</sup>

### Recommendations

- The Online Safety Codes should take the form of detailed prescriptive code encompassing both protective and preventive measures, prohibiting all forms of violence, exploitation and abuse; include child-friendly mechanisms for consultation and participation; provide support measures for parents and carers; and ensure effective remedies.<sup>55</sup>

---

<sup>47</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 38.

<sup>48</sup> *ibid* para 39.

<sup>49</sup> *ibid*.

<sup>50</sup> *ibid* para 73.

<sup>51</sup> Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5), 765–779. <<https://doi.org/10.1177/1461444816686327>> accessed 4 September 2023.

<sup>52</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 74.

<sup>53</sup> 5Rights Foundation, Making Child Online Safety a Reality: Global Toolkit (2022) 185.

<sup>54</sup> *ibid*.

<sup>55</sup> *ibid* para 73.

## Question 6: How should we design the Code to minimise the potential for conflict and maximise the potential for synergies in how platforms comply with it and the DSA?

 The Online Safety Code needs to be compatible with Ireland's International and Domestic Legislation. Of particular consideration should be the UN Conventions including the Convention on the Rights of the Child, the Irish Constitution and the European Convention on Human Rights.<sup>56</sup>

All public bodies in Ireland, including Coimisiún na Meán, have a responsibility to promote equality, prevent discrimination and protect the human rights of their service users and everyone affected by their policies and plans. This duty, known as the Public Sector Equality and Human Rights Duty, is located in section 42 of the Irish Human Rights and Equality Act 2014.

### Recommendations

- Ensure that when designing the Code that particular attention is paid to ensuring it is compliant with international and national human rights law.

---

<sup>56</sup> which has been incorporated into Irish Law by the European Convention on Human Rights Act 2003

## Question 7: To what extent, if at all, should the Code require VSPS providers to take measures to address content connected to video content?

We have heard from our members that the content connected to video content can often cause significant harm and distress to children and young people, particularly in the context of bullying. At times the video itself may not be the content that is causing harm but when it is considered alongside the content, such as comments connected to the video, it can cause significant distress and harm.<sup>57</sup> Our members have told us that Travellers and Roma are often targeted in the comments that go with particular videos (for example the poor treatment of animals) which can result in racist content being shared in the comments under the video content.<sup>58</sup>

### Recommendation

- Consideration should be given to requiring VSPS Providers to take measures to address content related to video content such as comments etc. This could include requiring VSPS providers to moderate content in comment sections, and have procedures in place for the timely removal of content.

---

<sup>57</sup> Children's Rights Alliance member consultation, August 2023.

<sup>58</sup> Communication received by the Children's Rights Alliance from Pavee Point, 25 August 2023.

## Question 8: How should we ask VSPS providers to introduce a feature that allows users to declare when videos contain advertising or other type of commercial communications? Should the Code include specific requirements about the form in which the declaration should take? What current examples are there that you regard as best practice?

User-created video content on social media platforms and video-streaming services (e.g., TikTok, YouTube) frequently involves commercial content and marketing messages. For example, unboxing videos, toy play videos or influencers reviewing products. It can be unclear for children and young people that this content is actually advertising.

The American Academy of Paediatrics has outlined that research on children's understanding of television advertising shows that:

- Children under the age of 8 have 'limited ability to understand the persuasive intent (i.e., that someone else is trying to change their thoughts and behaviour) of the advertiser.'
- Children aged 7 to 11 'can start to recognize television advertising and persuasive intent with their parents' assistance but lack the abstract thinking skills that help individuals recognize advertising as a larger commercial concept.'
- Children and young people over the age of 12 'were able to identify television advertisements (ads) and advertisers' intention to change behaviour'.<sup>59</sup>

The Council of Europe has recommended that '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'.<sup>60</sup>

The UN Committee on the Rights of the Child has reiterated this in their recent General Comment and has recommended that:

'States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes'.<sup>61</sup>

Aligned to this, the Committee have recommended that there is a need for the code to ensure that the profiling or targeting of children for commercial purposes is prohibited including practices that 'rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and

---

<sup>59</sup> The American Academy Of Pediatrics | Policy Statement, July 01 2020, Digital Advertising to Children, <<https://publications.aap.org/pediatrics/article/146/1/e20201681/37013/Digital-Advertising-to-Children?autologincheck=redirected>> accessed 29 August 2023.

<sup>60</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 20.

<sup>61</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 41

augmented reality environments to promote products, applications and services'.<sup>62</sup> The 2020 WHO-UNICEF-Lancet Commission on the future for the world's children noted that "commercial marketing of products that are harmful to children represents one of the most underappreciated risks to their health and wellbeing".<sup>63</sup>

Digital media advertising has changed dramatically over time and is predicted to account for 60% of global advertising expenditure by 2025.<sup>64</sup> A 2023 report from UNICEF and the WHO highlights that as marketing communication techniques have moved away from one-size-fits-all spot advertisements towards strategies for fostering engagement, children are now not just passive viewers of commercial messages, but rather 'active practitioners' in the commercial communications and marketing.<sup>65</sup>

## Recommendations

- The Code should look to ensure that a consistent feature for VSPS providers is introduced across all platforms that places a stringent requirement on users to declare when videos contain advertising and/or commercial communications. It should include a specific requirement for what form the declaration should take. This should be clear, concise, transparent and easy for children and young people to understand.

---

<sup>62</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 42.

<sup>63</sup> Clark, H., Coll-Seck, A.M., Banerjee, A., Peterson, S., Dalglish, S.L., Ameratunga, S. *et al.* (2020). A future for the world's children? A WHO-UNICEF-Lancet Commission. *Lancet* 2020; 395: 605-58. <[https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(19\)32540-1/fulltext#articleInformation](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(19)32540-1/fulltext#articleInformation)> accessed 4 September 2023.

<sup>64</sup> WHO, Understanding the digital media ecosystem. How the evolution of the digital marketing ecosystem impacts tobacco, alcohol and unhealthy food marketing (WHO 2022) <<https://apps.who.int/iris/handle/10665/355277>> accessed 4 September 2023.

<sup>65</sup> UNICEF and WHO, Taking action to protect children from the harmful impact of food marketing: a child rights-based approach. Geneva: World Health Organization and the United Nations Children's Fund (UNICEF 2023) 7.

## Question 9: How should we ask VSPS providers to introduce and design a flagging mechanism in the Code? How can we ensure that VSPS providers introduce the mechanism in a user-friendly and transparent way? How should we ask VSP Providers to report the decisions they've made on content after it has been flagged?

It should not be expected or assumed that a child will be able to identify or report content or conduct which are against a service's community guidelines. The 5Rights Foundation recommend having in place a number of moderation and reporting systems including take down mechanisms and flagging mechanisms.<sup>66</sup> Currently, there is no consistent flagging system in place for harmful content.

The best interest of the child should be a key focus when considering the design of the flagging mechanism in the code. The Council of Europe (COE) *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment* provide that 'in all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration' and further recommend that States should strike a balance between the child's right to protection and their other rights to freedom of expression, participation and access to information.<sup>67</sup> The COE also acknowledges the differing levels of maturity and understanding of children at different ages and recommends that States recognise the evolving capacities of children which can mean that the 'policies adopted to fulfil the rights of adolescents may differ significantly from those adopted for younger children'.<sup>68</sup>

An example of how to design a flagging mechanism that responds to the rights of children and young people can be seen in the UK Children's Code regarding the protection of children's data online. The code requires that designated services should provide 'prominent and accessible tools to help children exercise their data protection rights and report concerns.'<sup>69</sup> The ICO's guidance to services includes that the tools should be prominent and easy for the child to find, age appropriate and easy to use, tailored and specific to the rights they support, and include mechanisms for tracking progress and communicating with the service.<sup>70</sup> To make tools prominent the ICO suggests services highlight the reporting tools in their set up process and provide a clear icon on the screen display.<sup>71</sup> To make tools age appropriate and easy to use the ICO states that they should be tailored to the age of the child in question.<sup>72</sup> The ICO provide examples of how to do so in the Code for each age range from 0-5 up to 16-17.<sup>73</sup> In order to tailor their tools to support children's rights, the ICO suggest services create a 'download all my data' tool, a 'delete all my data tool' or 'select data for deletion' tool, a 'stop using my data' tool, and a 'correction' tool.<sup>74</sup> In terms of creating mechanisms that allow parents and children to track the progress of their flagged concern, the ICO state that information should be provided by the service about the timescales for responding to requests and these should be dealt with within the timescales set out at Article 12(3) of the GDPR.<sup>75</sup> Additionally, in order to

---

<sup>66</sup> 5Rights Foundation, 'But how do they know it is a child? Age Assurance in the Digital World'.

<sup>67</sup> Council of Europe, 'Recommendation 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' (COE 2018) <<https://bit.ly/2Xp9hpE>> accessed 26 February 2021, 12.

<sup>68</sup> *ibid.*

<sup>69</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' 8.

<sup>70</sup> *ibid.* 83-84.

<sup>71</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' 82.

<sup>72</sup> *ibid.*

<sup>73</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' 82-84.

<sup>74</sup> *ibid.* 84.

<sup>75</sup> *ibid.*

conform with the Code the ICO suggest that services should have mechanisms for children to indicate that they think their complaint or request is urgent, with appropriate prioritisation and the ability to take swift action on ongoing safeguarding issues.<sup>76</sup> This model could be taken and adapted to specifically relate to video content for the purposes of the Online Safety Code.

The DSA (Article 16) will require platforms to put in place a notification mechanism for illegal content and require them to process the notifications in a timely, diligent, non-arbitrary and objective manner. This should be integrated into the Code being developed. It is important to make the process for flagging content as straightforward and easy to understand for children and young people as possible. Children may find some of the rules set out in community guidelines confusing or struggle to distinguish between what is illegal and what is legal but prohibited by a service.<sup>77</sup> Requiring users to determine whether they are flagging content under the DSA or the Code would place a significant burden on the user and could act as a deterrent to children and young people flagging illegal and harmful online content.

## Recommendations

- Require VSPS to create a consistent flagging system for harmful content and introduce a number of moderation and reporting systems including take down mechanisms.
- The best interest of the child should be a key focus when considering the design of the flagging mechanism in the code.
- The DSA (Article 16) will require platforms to put in place a notification mechanism for illegal content and require them to process the notifications in a timely, diligent, non-arbitrary and objective manner. This should be integrated into the Code being developed.
- Flagging tools should be prominent and easy for the child to find, age appropriate and easy to use, tailored and specific to the rights they support, and include mechanisms for tracking progress and communicating with the service.

---

<sup>76</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' 84.

<sup>77</sup> Online abuse: teenagers might not report it because they often don't see it as a problem LSE blog by Powell-Jones. May 7th 2019.

## Question 10: What requirements should the Code include about age verification and age assurance? What sort of content should be shown by default to users who are logged out or in private browsing mode and whose age cannot be verified or assured? What evidence is there about the effectiveness of age estimation techniques? What current practices do you regard as best practice? Where accounts are not age verified should default privacy settings be used, should content default to universal content and should contact by others be more limited?

The use of age assurance ‘is not a silver bullet for keeping children safe online. It is simply a tool to identify that a service is dealing with a child.’<sup>78</sup> However, age assurance has the potential to drive the ‘development of new products and services to create a richer and more diverse digital ecosystem’ for children and young people rather than ‘being the route to keeping children out of the digital world’.<sup>79</sup>

The principle of data minimisation needs to be central to the design of any age assurance mechanism that is developed. The *Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment* state that age verification and assurance systems should use methods that are in line with the principle of data minimisation.<sup>80</sup> The UN Committee on the Rights of the Child has noted that ‘digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children’s right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives.’<sup>81</sup> Interference with a child’s right to privacy should only be permissible if it is ‘provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, be proportionate and designed to observe the best interests of the child’.<sup>82</sup>

There needs to be a range of age assurance solutions developed that can respond to the different situations that children and young people face.<sup>83</sup> The 5Rights Foundation have set out that ‘many of the changes necessary to make a service age appropriate do not need additional or new age assurance technologies, but rather require services to disable some of their more intrusive or risky design features’.<sup>84</sup>

There is a need to ensure that there are minimum standards put in place for age assurance. This could include ‘an explicit risk-based framework that would allow businesses to understand what level of assurance is required in different scenarios.’<sup>85</sup>

---

<sup>78</sup> 5Rights Foundation, ‘But how do they know it is a child? Age Assurance in the Digital World’ 7.

<sup>79</sup> *ibid* 9.

<sup>80</sup> Council of Europe, *Guidelines to respect, protect and fulfil the rights of the child in the digital environment* (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 69.

<sup>81</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 68.

<sup>82</sup> *ibid*.

<sup>83</sup> 5Rights Foundation, ‘But how do they know it is a child? Age Assurance in the Digital World’ 7.

<sup>84</sup> 5Rights Foundation, ‘Pathways: How digital design puts children at risk’ 11.

<sup>85</sup> *ibid*.

5Rights Foundation have set out 11 common standards that should inform the development of any age assurance mechanism including:

- Age assurance must be privacy preserving.
- Age assurance should be proportionate to risk and purpose.
- Age assurance should be easy for children to use.
- Age assurance must enhance children’s experiences, not merely restrict them.
- Age assurance providers must offer a high level of security.
- Age assurance providers must offer routes to challenge and redress.
- Age assurance must be accessible and inclusive.
- Age assurance must be transparent and accountable.
- Age assurance should anticipate that children don’t always tell the truth.
- Age assurance must adhere to agreed standards.

Age assurance must be carried out in compliance with children’s rights under National and International law. In order to ensure a rights-based approach to the design and implementation of age assurance measures a human rights analysis should be carried out and measures that are compliant with children’s rights should be adopted. The level of assurance should be proportionate to the nature and level of risk presented by a product or service in relation to the age of the child. It is important that the ‘cumulative nature of risk must also be taken into account, as multiple design features or different parts of a user’s journey combine to create greater risks.’<sup>86</sup>

#### *United Kingdom Children’s Code*

The UK Children’s Code regarding the protection of children’s data online, offers a dual option to designated services in order to comply with the standard of age verification or ‘age appropriate application’ as it is termed under the Code. Under the Code designated services are required to take a risk-based approach to recognising the age of individual users either by establishing age ‘with a level of certainty that is appropriate to the risks to the rights and freedoms of children that have arisen from [their] data processing’ or by applying the standards in the Code to all users.<sup>87</sup> The ICO suggest that Data Protection Impact Assessments (DPIA), which are set out at Standard 2 in the Code, should be used to aid this assessment.<sup>88</sup> The Code is not prescriptive about the exact methods services should use to establish age or the level of certainty provided focussing instead on the need to use a method that is appropriate to the risk level involved from the service’s data processing.<sup>89</sup> However, the ICO does provide a non-exhaustive list of options for services to consider including self-declaration, artificial intelligence, third party verification services, account holder confirmation,

---

<sup>86</sup> *ibid* 19.

<sup>87</sup> Information Commissioner’s Office, ‘Age Appropriate Design: A Code of Practice for Online Services’ 32.

<sup>88</sup> *ibid*.

<sup>89</sup> Information Commissioner’s Office, ‘Age Appropriate Design: A Code of Practice for Online Services’ 33.

technical measures, and hard identifiers.<sup>90</sup> The ICO assesses whether a service has chosen the appropriate method by taking account of the products available on the market currently, and in particular for small businesses which cannot develop their own age verification tool due to capacity and resource constraints.<sup>91</sup> Guidance is provided in the Code on how to uphold rights if the collection of personal data is required in order to establish age.<sup>92</sup> The ICO stresses that while there are tensions between age assurance and compliance with the GDPR, age assurance and the GDPR are compatible if privacy by design solutions are used.<sup>93</sup>

## Recommendations

- Age verification and assurance mechanisms should respect the principle of data minimisation and avoid unlawful or arbitrary interference with the right of the child to privacy.
  - Ensure that any age assurance mechanism introduced is compliant with children's rights under National and International law.
  - There should be a range of age assurance solutions developed which respond to the different situations children and young people face.
  - Ensure that there are minimum standards put in place for age assurance. This could include an explicit risk-based framework that would allow businesses to understand what level of assurance is required in different scenarios.
- Data Protection Impact Assessments and Children's Rights Impact Assessments could be used to monitor the level of interference of age verification mechanisms with the right of the child to privacy and help balance that right with the need for protection online.

---

<sup>90</sup> *ibid* 34.

<sup>91</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' 33.

<sup>92</sup> *ibid* 35.

<sup>93</sup> *ibid*.

## Question 11: What requirements should the Code have in relation to content rating? What do you consider to be current best practice? What experiences have you had using content rating systems on platforms and do you think they have been effective? What steps could we ask VSPS to take to ensure content is rated accurately by users?

The UN Committee on the Rights of the Child has recommended that States ‘should encourage providers of digital services used by children to apply concise and intelligible content labelling, for example on the age-appropriateness or trustworthiness of content.’<sup>94</sup> The Council of Europe has recommended that ‘states should co-operate with a view to promoting standardisation of content classification and advisory labels among countries and across stakeholder groups to define what is appropriate and what is inappropriate for children.’<sup>95</sup> There are a number of frameworks that could be considered.

A key tool to identify risk and classification of harm is the 4Cs framework. This framework should be considered for adoption in the Online Safety Code.

The CO:RE 4Cs classification recognises that online risks arise when a child:

- Engages with and/or is exposed to potentially harmful content
- Experiences and/or is targeted by potentially harmful contact
- Witnesses, participates in and/or is a victim of potentially harmful conduct
- Is party to and/or exploited by a potentially harmful contract<sup>96</sup>

The 4Cs classification ‘distinguishes between aggressive, sexual and value risks’ along with recognising important cross-cutting risks such as children’s right to privacy and fair treatment.<sup>97</sup>

---

<sup>94</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 55.

<sup>95</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 29, para 121.

<sup>96</sup> CORE, ‘4 Cs of online risk: Short report & blog on updating the typology of online risks to include content, contact, conduct, contract risk’ <<https://core-evidence.eu/posts/4-cs-of-online-risk>> accessed 28 August 2023.

<sup>97</sup> *ibid.*

 CORE	<b>Content</b> Child as recipient	<b>Contact</b> Child as participant	<b>Conduct</b> Child as actor	<b>Contract</b> Child as consumer
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
<b>Sexual</b>	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
<b>Values</b>	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
<b>Cross-cutting</b>	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

98

A classification scheme is in place in Australia where the Australian Online Safety Act (2021) defines content as either ‘class 1 material’ or ‘class 2 material’.<sup>99</sup> Class 1 material and class 2 material are defined by reference to Australia’s National Classification Scheme, which is also used for classification of films, computer games and other publications.

Class 1 material includes material that:

- ‘depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence.’

Class 2 material is material that is, or would likely be, classified as either:

- ‘X18+ (or, in the case of publications, category 2 restricted), or
- R18+ (or, in the case of publications, category 1 restricted) under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old.’

The eSafety Commissioner works with online service providers to ensure access to Class 2 material, which is considered unsuitable for children and young people under 18, is restricted.

<sup>98</sup> CORE, ‘4 Cs of online risk: Short report & blog on updating the typology of online risks to include content, contact, conduct, contract risk’ <<https://core-evidence.eu/posts/4-cs-of-online-risk>> accessed 28 August 2023.

<sup>99</sup> Online Safety Act 2021 s106 and s107.

## Recommendations

- Content labelling should be concise, intelligible and written in child friendly language.
- Consider adopting the 4C's classification framework for content labelling for child safety online.

## Question 12: What requirements should the Code have in relation to parental control features? How can we ensure that VSPS providers introduce the mechanism in a user-friendly and transparent way? Can you point to any existing example of best practice in this area? Should parental controls be ‘turned-on’ by default for accounts of minors or where age is not verified?

While parental controls are one measure for protecting children online they ‘are not a substitute for good design that prioritises user safety’ and can result in parents having a false sense of security ‘while children continue to be exposed to risks due to poor service design’.<sup>100</sup> The most vulnerable children offline are often the most vulnerable online also. Parental control features and safety features have to take this into account as parents may not be in a position to protect their child online.

The Council of Europe has recommended that children’s evolving capacities should be taken into account when businesses establish or update their parental controls.<sup>101</sup> Additionally, States should ensure that such controls do not reinforce discriminatory attitudes or infringe on children’s privacy and information rights.<sup>102</sup>

The UK Children’s Code specifies that if a regulated service provides parental controls, they should give the child age appropriate information about this.<sup>103</sup> If the regulated service allows a parent or carer to monitor their child’s activity online or track their location then they should provide an obvious sign to the child when they are being monitored.<sup>104</sup> ICO ground the basis for this standard within the best interests of the child principle in Article 3 UNCRC, the right of the child to privacy under Article 16, and the requirement under Article 5(1)(a) of the GDPR that any processing of personal data must be lawful, fair and transparent. In terms of conforming to the standard, regulated services should also provide parents with information about the child’s right to privacy and resources for age appropriate discussion between parent and child.<sup>105</sup> The ICO also provide a table with some indicative measures that services could take to ensure compliance that are appropriately targeted at each age group.<sup>106</sup> The Code regulates where a service has parental controls in place but does not require services to have such controls in place.

VSPS must be careful if introducing parental controls to ensure that they do so in a balanced manner that respects the autonomy and privacy rights of the child, cognisant of their developing capacity while also balancing their best interests and safeguarding concerns. The new Online Safety Code should provide guidance on best practice for those services that decide to introduce parental controls.

### Recommendations

- Parental Controls should not be a substitute for safety by design features.

---

<sup>100</sup> [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0027/226269/5rights-foundation.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0027/226269/5rights-foundation.pdf).

<sup>101</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 54.

<sup>102</sup> *ibid.*

<sup>103</sup> Information Commissioner’s Office, ‘Age Appropriate Design: A Code of Practice for Online Services’ 61.

<sup>104</sup> *ibid.*

<sup>105</sup> Information Commissioner’s Office, ‘Age Appropriate Design: A Code of Practice for Online Services’ 62.

<sup>106</sup> *ibid.*

- Where parental controls are adopted, they should respect and reflect the evolving capacities of the child and be compatible with human rights and privacy law.
- Where parental controls are used by a VSPS children and young people who are service users should be given age appropriate and accessible information about this.
- Regulated services should provide parents with information about the child's right to privacy and resources for age appropriate discussion between parent and child.

## Question 13: What requirements should the Code contain to ensure that VSPS provide for effective media literacy measures and tools?

Digital and media literacy is an area that requires specific and targeted measures<sup>107</sup> to ensure equal access to the digital environment and the full realisation of children's rights. The UN Committee on the Rights of the Child have stated that parents and guardians should be supported to gain digital literacy in order to support their children in traversing the digital environment in a way which respects their evolving capacities,<sup>108</sup> and educational programmes and materials should be provided in order to develop digital literacy skills.<sup>109</sup> In order to support the full breadth of children's rights, digital literacy education should include both functional and technical competencies, skills related to content creation, and critical thinking around the impacts of the digital environment.<sup>110</sup>

Digital and media literacy programmes must be accessible to all groups and in particular the most vulnerable. Travellers experience low levels of literacy and low levels of media literacy as a result of exclusion within the education system resulting in low levels of school completion.<sup>111</sup> Roma experience similarly low levels of media literacy and also face language barriers.<sup>112</sup> It is therefore vital that groups such as Travellers and Roma are targeted by VSPS in terms of media literacy measures and tools. It is important that Traveller parents are empowered in relation to parental controls and other controls and tools that may be available to them. This needs to happen in a culturally appropriate way and in consultation with Traveller organisations. Additionally, children who lack resources at home or live in residential care should not be disadvantaged from accessing digital literacy opportunities.<sup>113</sup>

Particular efforts should be made to reach those children who have no access to digital technology due to socio-economic or geographic reasons, and those who have access but lack the skills to use or underuse technology due to vulnerability or disability.<sup>114</sup> Effective digital literacy should enhance and promote the equality of opportunity and outcomes for all and in particular should promote gender equality by enhancing the use of technology by girls.<sup>115</sup> Educational programmes and resources on digital literacy should include information on preventive measures, rights and responsibilities in the digital environment, risk and violation identification, and effective remedies.<sup>116</sup> These programmes should enable children to respect fundamental rights, understand what it means to give consent, enable an understanding of what constitutes and how to deal with harmful content including how to seek redress, and to understand the potential consequences of sharing personal information online.<sup>117</sup>

---

<sup>107</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 11.

<sup>108</sup> *ibid*, para 21.

<sup>109</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 32.

<sup>110</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 42.

<sup>111</sup> Pavee Point, Submission to Coimisiún na Meán Call For Inputs on Developing First Online Safety Code 2023.

<sup>112</sup> *ibid*.

<sup>113</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 44.

<sup>114</sup> *ibid* 45.

<sup>115</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 46.

<sup>116</sup> *ibid* 48.

<sup>117</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 48.

## Recommendations

- Digital literacy education should include both functional and technical competencies, skills related to content creation, and critical thinking around the impacts of the digital environment.
- Parents and guardians should be supported to gain digital literacy in order to support their children in traversing the digital environment in a way which respects their evolving capacities.
- Digital literacy programmes must be accessible to all groups and in particular the most vulnerable.
- Educational programmes and resources on digital literacy should include information on preventive measures, rights and responsibilities in the digital environment, risk and violation identification, and effective remedies.

## Question 14: How should key aspects of terms and conditions be brought to users' attention? What examples are there of best practice in relation to terms and conditions including content moderation policies and guidelines?

Terms and conditions should be accessible, transparent, fair, and available in child friendly language and recognising that parents and guardians may rely on such terms and conditions as a guide to the suitability of content for their children, businesses should take reasonable steps to ensure they are enforced.<sup>118</sup>

It is important that published terms:

- use simple language
- aid comprehension
- be concise
- be presented in multiple formats for different age ranges
- be prominent and easy to find
- be presented at the right moments in a user journey
- consider the diverse needs of young people
- not assume adult involvement
- cater for children with accessibility needs
- ensure that consent must be obtained and sought, not assumed
- ensure users are given meaningful choices<sup>119</sup>

Alongside this the Code should ensure that:

- Terms of agreement should be proportionate to the value young people derive from the service
- Terms of service must be consistently enforced
- Rules must be harmonised and consistent with relevant regulation
- Terms must set out clear rules for what constitutes a breach of terms
- Terms and conditions must clarify what happens when a user makes a complaint<sup>120</sup>

---

<sup>118</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 14, 97.

<sup>119</sup> 5Rights Foundation, Tick to Agree Age appropriate presentation of published terms September 202, 10-22.

<sup>120</sup> ibid 22-32.

In the UK Children’s Code under the transparency standard, the ICO state that if designated services need to draft their terms and conditions in a certain way to be legally robust then they can provide child-friendly explanations in order to meet the standard of providing clear terms, policies and community standards.<sup>121</sup>

### Recommendations

- Terms and conditions should be accessible, transparent, fair, and available in child friendly language.
- Terms of agreement should be proportionate to the value young people derive from the service.
- Terms of service must be consistently enforced and set out clear rules for what constitutes a breach.
- Terms and conditions should be drafted in child friendly and plain language. If this is not possible services should provide additional child friendly explanations in order to provide clear terms and policies.

---

<sup>121</sup> Information Commissioner’s Office, ‘Age Appropriate Design: A Code of Practice for Online Services’ 39.

## Question 15: How should we ask VSPS providers to address content moderation in the Code? Are there any current practices which you consider to be best practice? How should we address automated content detection and moderation in the Code?

The UN Committee on the Rights of the Child has recommended that ‘Content moderation and content controls should be balanced with the right to protection against violations of children’s other rights, notably their rights to freedom of expression and privacy.’<sup>122</sup> Further the Committee has stated that State Parties ‘should ensure that digital service providers comply with relevant guidelines, standards and codes and enforce lawful, necessary and proportionate content moderation rules.’<sup>123</sup> On automated systems the Committee has recommended that States ‘should ensure that uses of automated processes of information filtering, profiling, marketing and decision-making do not supplant, manipulate or interfere with children’s ability to form and express their opinions in the digital environment.’<sup>124</sup> The Committee also notes that ‘automated systems may be used to make inferences about a child’s inner state’ and that States should ‘ensure that automated systems or information filtering systems are not used to affect or influence children’s behaviour or emotions or to limit their opportunities or development.’<sup>125</sup>

It is essential that services are not allowed to rely solely on user complaints and are obliged to engage in proactive moderation practices. The 5Rights Foundation have noted that ‘proactive moderation lifts the burden off children to flag and report content and behaviour that violates a service’s community guidelines.’<sup>126</sup>

The Code should ensure that moderation is ‘proportionate to the risk and activities associated with the product or service.’<sup>127</sup> This would mean that services which are directed at children and young people ‘should pre-moderate all user-generated content’ and services with varied audiences ‘should offer children a higher bar of moderation than other users.’<sup>128</sup>

Moderation must be fair, unbiased and consistent for it to be effective.<sup>129</sup> The Online Safety Code presents an opportunity for providers to be held to ‘agreed enforceable standards of moderation, including oversight of automated decisions and training and care for human moderators’.<sup>130</sup>

### Recommendations

- Content moderation and content controls should be balanced with the right of the child to privacy and freedom of expression.
- Content moderation rules should be necessary and proportionate to the risk and activities associated with VSPS products or services.

---

<sup>122</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 58.

<sup>123</sup> *ibid.*

<sup>124</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 61.

<sup>125</sup> *ibid* para 62.

<sup>126</sup> 5Rights Foundation, Tick to Agree Age appropriate presentation of published terms September 2021, 34.

<sup>127</sup> *ibid.*

<sup>128</sup> 5Rights Foundation, Tick to Agree Age appropriate presentation of published terms September 2021, 34.

<sup>129</sup> *ibid.*

<sup>130</sup> 5Rights Foundation, Tick to Agree Age appropriate presentation of published terms September 2021, 35.

- Automated system should not be used to affect or influence children's behaviour or emotions.
- Services directed at children and young people should pre-moderate all user-generated content and services with a varied audience should offer children and young people a higher bar of moderation than other users.
- Moderation should be fair, unbiased, and consistent.

## Question 16: What requirements should the Code include about procedures for complaint-handling and resolution, including out-of-court redress or alternative-dispute resolution processes? How frequently should VSPS providers be obliged to report to the Commission on their complaint handling systems and what should those reports contain? Should there be a maximum time-period for VSPS providers to handle user complaints and if so, what should that period be?

The UN Committee on the Rights of the Child recommended in its 2021 General Comment that ‘States parties should ensure that appropriate and effective remedial judicial and non-judicial mechanisms for the violation of children’s rights relating to the digital environment are widely known and readily available to all children and their representatives’.<sup>131</sup> The Committee also recommended that ‘complaint and reporting mechanisms should be free of charge, safe, confidential, responsive, child-friendly and available in accessible formats.’<sup>132</sup> The Committee is clear that in order to protect children there is a need for complaint handling to be ‘swift to halt any ongoing and future damage.’<sup>133</sup>

In 2018, the Council of Europe published its Recommendation, *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment* which recommends that States require businesses to meet their responsibilities by requiring them to implement measures and ‘encourage them to co-operate’ with the State and other stakeholders, including children.<sup>134</sup> It further recommends that Member States should ensure that a child’s right to an effective remedy under the European Convention of Human Rights<sup>135</sup> is respected and protected when their rights have been infringed online.<sup>136</sup> This means that States are required to make provision for ‘known, accessible, affordable, and child-friendly avenues through which children, as well as their parents or legal representatives, may submit complaints and seek remedies’.<sup>137</sup> States and relevant stakeholders such as VSPS should provide children with information in a manner that they can understand on complaints processes and handling so that they are enabled to exercise their participation rights fully.<sup>138</sup> Guidance is given on what constitutes an effective remedy and it includes:

- inquiry,
- explanation,

---

<sup>131</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 44.

<sup>132</sup> *ibid.*

<sup>133</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 46.

<sup>134</sup> Council of Europe, ‘Recommendation 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’ (COE 2018) 11.

<sup>135</sup> European Convention of Human Rights Art 6 and 19.

<sup>136</sup> Council of Europe, ‘Recommendation 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’ (COE 2018) 24.

<sup>137</sup> *ibid.*

<sup>138</sup> Council of Europe, ‘Recommendation 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’ (COE 2018) 5.

- reply,
- correction,
- proceedings,
- immediate removal of unlawful content,
- apology,
- reinstatement,
- reconnection
- compensation.<sup>139</sup>

Importantly, it provides that the process should be speedy, child-friendly and provide the appropriate redress.<sup>140</sup> In order to be effective it is essential that the Codes provide for a maximum time-period for VSPS providers to handle user complaints that offers and quick and effective resolution for children and young people. The Online Safety Code developed by the Australian eSafety Commissioner states that Tier 1 social media services must resolve complaints within ‘a reasonable time’ and that what constitutes a reasonable time ‘should be based on the scope and urgency of potential harm that is related to a complaint and the source of the complaint.’<sup>141</sup>

It is important that VSPS providers are required to be transparent in their complaint handling. To this end they should be required to report on their complaint handling systems at a minimum annually.

### Recommendations

- Complaint and reporting mechanisms should be free of charge, safe, confidential, responsive, child-friendly and available in accessible formats.
- VSPS should provide children with information in a manner that they can understand on complaints processes and handling.
- The new Online Safety Code should provide for a maximum time-period for VSPS providers to handle user complaints that offers and quick and effective resolution for children and young people and guidance as to what is a reasonable timeframe for responding to complaints.

---

<sup>139</sup> *ibid.*

<sup>140</sup> *ibid.*

<sup>141</sup> eSafety Commissioner for Australia, Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material), 15.

## Question 17: What approach do you think the Code should take to ensuring that the safety measures we ask VSPS providers to take are accessible to people with disabilities?

The UN Committee on the Rights of the Child has noted that children with disabilities may be ‘more exposed to risks, including cyberaggression and sexual exploitation and abuse, in the digital environment.’<sup>142</sup> The Committee recommends that states take measures to identify the risks faced by children with disabilities and take steps to ensure they are safe in the digital environment.<sup>143</sup> This should be done in a way that counters ‘prejudice faced by children with disabilities that might lead to overprotection or exclusion.’<sup>144</sup> It is important that information is provided in accessible formats on safety and protective strategies.<sup>145</sup> One method of ensuring this is equality proofing safety measures and providing guidance on various accessibility methods in place.<sup>146</sup>

The Code must respect the evolving capacities of all children including those of children with disabilities or in vulnerable situations.<sup>147</sup> Policies and practices adopted by VSPS under the Code must respect and respond to the needs of these groups in the digital environment and reflect appropriately the differing needs of children of different ages and backgrounds.<sup>148</sup>

### Recommendations

- Information should be provided in accessible formats on safety and protection strategies.
- Safety measures should be equality proofed as a matter of standard practice.
- Policies and practices adopted by VSPS under the Code must respect and respond to the needs of children and young people with disabilities in the digital environment and reflect appropriately the differing needs of children of different ages and backgrounds.

---

<sup>142</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 92.

<sup>143</sup> *ibid.*

<sup>144</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, para 92.

<sup>145</sup> *ibid.*

<sup>146</sup> For information on equality proofing see: S. Cantillon, K. Lynch, J. Baker, A. Connelly, ‘a Framework for Equality Proofing: A Paper Prepared for the National Economic and Social Forum’ 1995, [A framework for equality proofing: a paper prepared for the national economic and social forum — ResearchOnline \(gcu.ac.uk\)](#).

<sup>147</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 2.

<sup>148</sup> *ibid.*

## Question 18: What approach do you think the Code should take to risk assessments and safety by design? Are there any examples you can point us towards which you consider to be best practice?

In 2018, the Council of Europe published its Recommendation, *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment* and noted that the online world is reshaping children's lives in many ways, resulting in 'opportunities for and risks to their well-being and enjoyment of human rights.'<sup>149</sup> Recognising that businesses have a responsibility to respect children's rights,<sup>150</sup> the Council of Europe recommends that States require businesses to meet their responsibilities by compelling them to implement measures and 'encourage them to co-operate' with the State and other stakeholders, including children.<sup>151</sup> A key proposal of these Guidelines is that States should require relevant stakeholders to implement safety by design, privacy by design and privacy by default measures, taking into account the best interests of the child.<sup>152</sup> Including these principles in the Online Safety Code would help ensure that, from the planning stages of technology development onward, children are protected. The UN Committee on the Rights of the Child in 2021 recommended that that States should incorporate 'the integration of privacy-by-design into digital products and services that affect children.'<sup>153</sup>

Many of the digital services children and young people use are not designed to protect their rights or meet their needs.<sup>154</sup> Research from the 5Rights Foundation found that 'pathways designed into digital services and products are putting children at risk' with designers tasked with 'optimising products and services for three primary purposes, all geared towards revenue generation.'<sup>155</sup> The Online Safety Code presents a huge opportunity to embed the principle of safety by design into the Irish regulatory framework. It is important that this principle is not incorporated only to services specifically targeted to children and young people but to all the digital services children and young people are likely to actually access.<sup>156</sup>

The *Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment* state that States should require businesses to regularly undertake child-rights impact assessments in relation to digital technologies and demonstrate that they are taking reasonable steps to mitigate risks.<sup>157</sup> Child rights risk assessments should be conducted by business "before their digital products or services could reach or affect children"<sup>158</sup> and businesses should be obliged to "undertake child rights due diligence, which entails that businesses should identify, prevent, and

---

<sup>149</sup> Council of Europe, 'Recommendation 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' (COE 2018) 10.

<sup>150</sup> UN Committee on the Rights of the Child, General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights CRC/C/GC/16.

<sup>151</sup> Council of Europe, 'Recommendation 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' (COE 2018) 11.

<sup>152</sup> *ibid* 23.

<sup>153</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 70.

<sup>154</sup> 5Rights Foundation, 'Design of Service' <<https://5rightsfoundation.com/our-work/design-of-service/>> accessed 4 September 2023

<sup>155</sup> 5Rights Foundation, September 2021 Pathways: A Summary Key findings and recommendations from Pathways: How digital design puts children at risk

<sup>156</sup> 5Rights Foundation, 'Design of Service' <<https://5rightsfoundation.com/our-work/design-of-service/>> accessed 4 September 2023

<sup>157</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 95.

<sup>158</sup> The Handbook for policy-makers on the rights of the child in the digital environment by the Council of Europe that accompanies the Recommendation (Livingstone et al., 2020,) 19

mitigate their impact on children’s rights including across their business relationships and within global operations.”<sup>159</sup>

### Recommendations

- The requirement of safety by design should be one of the key measures included in the Online Safety Code and it should require safety by design to be implemented as standard into all products and services of VSPS.
- Child rights risk assessments should be conducted by VSPS before their digital products or services could reach or affect children.
- VSPS should regularly undertake children’s rights impact assessments in relation to digital technologies and demonstrate that they are taking reasonable steps to mitigate risks.

---

<sup>159</sup> ibid 72.

## Question 19: How do you think that cooperation with other regulators and bodies can help us to implement the Code for VSPS?

Cooperation with other regulators could form an important support for implementation of the Code across key areas of accessibility, human rights compliance and child safety.

In terms of child safety and participation, Tusla could provide an insight on the issues faced by children and young people it works with, and the formal child consultation units in the Department of Children, Equality, Disability, Integration and Youth (DCEDIY) could be coordinated with to ensure proper consultation and engagement from young people on the Code and its implementation.

In terms of human rights compliance and implementation of the public sector duty, the Irish Human Rights and Equality Commission (IHREC) could advise on best practice.

To ensure robust accessibility measures in the development and implementation phases of the Code, the Disability Authority should be coordinated with.

### Recommendations

- Cooperate with other public bodies and government departments including Tusla, IHREC, DCEDIY, and the Disability Authority in order to ensure effective implementation of the new Online Safety Code.

## Question 21: Do you have any views on how requirements for commercial content arranged by a VSPS provider itself should be reflected in the Code?

Consideration should be given to addressing Harmful Commercial Communications, particularly marketing of high fat, sugar and salt foods and breastmilk substitutes and alcohol.

The American Academy of Paediatrics has outlined that research on children's understanding of television advertising shows that:

- Children under the age of 8 have 'limited ability to understand the persuasive intent (i.e., that someone else is trying to change their thoughts and behaviour) of the advertiser.'
- Children aged 7 to 11 'can start to recognize television advertising and persuasive intent with their parents' assistance but lack the abstract thinking skills that help individuals recognize advertising as a larger commercial concept.'
- Children and young people over the age of 12 'were able to identify television advertisements (ads) and advertisers' intention to change behaviour'.<sup>160</sup>

The Council of Europe has recommended that '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.'<sup>161</sup>

The UN Committee on the Rights of the Child has reiterated this in their recent General Comment and has recommended that:

'States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes.'<sup>162</sup>

Aligned to this, the Committee have recommended that there is a need for the code to ensure that the profiling or targeting of children for commercial purposes is prohibited including practices that 'rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services'.<sup>163</sup>

### Recommendations

- Consideration should be given to addressing Harmful Commercial Communications, particularly marketing of high fat, sugar and salt foods, breastmilk substitutes and alcohol.

---

<sup>160</sup> The American Academy Of Pediatrics | Policy Statement, July 01 2020, Digital Advertising to Children, <<https://publications.aap.org/pediatrics/article/146/1/e20201681/37013/Digital-Advertising-to-Children?autologincheck=redirected>> accessed 29 August 2023.

<sup>161</sup> Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018) Recommendation CM/Rec(2018)7 of the Committee of Ministers, 20.

<sup>162</sup> UN Committee on the Rights of the Child, General Comment no 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, para 41.

<sup>163</sup> ibid para 42.

- VSPS 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.
- The best interests of the child should form a primary consideration when regulating advertising and marketing addressed to and accessible to children.
- Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes.
- The profiling or targeting of children for commercial purposes should be prohibited.

## Question 23: Should the Code have a transition period or transition periods for specific issues? What time frame would be reasonable for a transition period?

It is important that the Online Safety Code comes into force as soon as is possible without delay. Currently platforms are largely unregulated with children and young people experiencing harm online daily. In 2021, CyberSafeKids reported that a quarter of all children have seen or experienced something online in the last year that bothered them, with almost one third of those children having kept it to themselves rather than report it to their parents or someone else.<sup>164</sup>

The transition period should be as short as possible to ensure that there is robust protection for children and young people in the digital space. A useful example is the UK Children's Code which provided for a one-year transition period to encourage conformance.<sup>165</sup> For pre-existing services, the Code recommended some measures to take including reviews of processing and pre-existing data protection impact assessments during this period as well as assessing any additional measures that would be needed to conform to the Code.<sup>166</sup> A timeframe like this could be considered.

### Recommendations

- It is important that the Online Safety Code comes into force as soon as is possible without delay and the transition period should be as short as possible to ensure that there is robust protection for children and young people in the digital space.

---

<sup>164</sup> CyberSafeKids, *Annual Report 2021 (2022)* 3.

<sup>165</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services' 21.

<sup>166</sup> *ibid.*