

# Response to the Revised Online Safety Code

August 2024



Founded in 1995, the Children's Rights Alliance unites over 150 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.

A.S.S.C Accompaniment Support Services for Children  
Alcohol Action Ireland  
Amber Women's Refuge  
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  
Bedford Row Family Project  
BeLonG To Youth Services  
Bodywhys  
Breaking Through CLG  
Catholic Guides of Ireland  
Child Law Project  
Childhood Development Initiative  
Children in Hospital Ireland  
Children's Books Ireland  
Children's Grief Centre  
ChildVision  
Citywise Education  
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  
Empowerment Plus  
EPIC  
Extern Ireland  
FamiliBase  
Féach  
Focus Ireland  
Foróige  
Gaeloideachas  
Galway Traveller Movement  
GIY Ireland  
Good Shepherd Cork  
Helium Arts  
Humanist Association of Ireland  
Immigrant Council of Ireland  
Inclusion Ireland  
Inner City Organisations Network (ICON)  
Institute of Guidance Counsellors  
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  
Laois Domestic Abuse Services  
Leap Ireland  
Let's Grow Together  
LGBT Ireland  
Meath Women's Refuge & Support Services  
Mecpaths  
Mental Health Reform  
Mercy Law Resource Centre  
Migrant Rights Centre Ireland  
Mothers' Union  
Move Ireland  
Museum of Childhood Ireland  
Music Generation  
My Mind  
My Project Minding You  
National Childhood Network  
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  
Our Lady of Lourdes Community Services Group  
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  
SAFE Ireland  
Saoirse Domestic Violence Services  
SAOL Project  
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  
StartBright Early Learning Centres  
TASC  
Teachers' Union of Ireland  
Teach Tearmainn  
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  
Troiir  
UNICEF Ireland  
Variety – the Children's Charity of Ireland  
Vision Ireland  
Women's Aid  
YMCA Dublin  
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)

© 2024 Children's Rights Alliance – Republic of Ireland Limited  
The Children's Rights Alliance is a registered charity – CHY No. 11541

## Executive Summary

---

The Revised Audio-Visual Media Services Directive (EU) 2018/1808 and the Audio-Visual Media Services regulation Act 2022 serve as the legislative foundation for the Code. At the Alliance, we also recognise the relevance of the Digital Services Act and the overlap and mutuality between these frameworks.

### Key Concerns

Despite the Revised Code's improvements, the Alliance is concerned about the Code's ability to effectively protect children and young people from online audiovisual content in the following areas which are outlined fully in our submission.

**Inadequate Protection Measures for Children and Young people:** The Code falls short of meeting the obligations under Article 28b(1)(a) of Directive (EU) 2018/1808, which mandates appropriate measures be taken to protect children from content which may impair their physical, mental or moral development. The Code has interpreted this obligation narrowly, resulting in insufficient protections.

**Definition and Regulation of Content:** The shift from 'regulated content harmful to children' to 'restricted content' dilutes the focus on child-specific risks, which in turn limits the effectiveness of the responses required by platforms in discharging their duties to safeguard the rights of children. In particular, the implications this may have in how the 'risk-test' is interpreted and applied, and the absence of any requirement to prioritise content flagged by or involving children. Additionally, the absence of a definition of 'pornography', further weakens the Code's effectiveness.

**Age Verification and Assurance:** The Code's age verification requirements are largely limited to adult-only content (narrowly defined) and lacks any robust measures to protect children from harms they may encounter on AVMS platforms that do *not* permit 'adult-only content', but whose platforms still contain harmful content (most online platforms). This greatly limits the ability to prevent children and young people from being exposed to these harms. The limited requirement for age verification (only explicitly for adult-only sites) does not go far enough in requiring platforms to ensure that underage and child users cannot create and use online platforms or in determining what may be 'age-appropriate content'.

**Recommender Systems:** The exclusion of recommender system regulations overlooks the harm caused by algorithms that expose children to inappropriate content. The Alliance advocates for the regulation of recommender systems to ensure these systems do not impair the physical, mental or moral development of children and young people. There is no conflict or parallel regulation between the DSA and the Directive, as both apply in Ireland under EU law, which cannot conflict with itself. These interlocking pieces of legislation, along with the 2022 Act, form a mutually reinforcing framework aimed at enhancing online safety.

**Removal of Offence-Specific Harms from the Code:** The removal of offence-specific harms from the Code does not adequately address illegal content specific to children, such as grooming or engaging with a child for the purposes of child sexual abuse. The Alliance is of

the view that offence-specific harms involving children should be included in the Code to ensure that platforms are explicitly and clearly required to restrict and preclude users from engaging with children to induce them into uploading or sharing content that is an offence in Irish law that involves or impacts a child or children. Furthermore, the inclusion would also have the benefit of supporting the implementation and effectiveness of the DSA.

**Parental Controls and Privacy:** While parental controls are included, they are limited to users under 16 years. Also, the Code does not mandate privacy-by-design measures for children's accounts. The Alliance highlights the necessity for the Code to require default privacy settings for all user who are under 18 years to protect children's data and ensure safer online interactions.

**Complaints and Enforcement Mechanisms:** The Code lacks specific requirements for age-appropriate and accessible complaint mechanisms. There is no obligation for priority handling of complaints involving children, nor is there a mandate for providers to expedite child-related complaints.

## Recommendations

The Alliance acknowledges the positive steps taken in the Revised Online Safety Code but maintains that further enhancements are necessary to fully protect children's rights online:

### Age Verification:

- **Effective Age Assurance Measures:** The Code should provide for a clear obligation on what constitutes an effective age assurance measure to include a quantifiable benchmark.
- **Comprehensive Age Assurance Implementation:** The Code should extend age assurance requirements beyond adult-only content to ensure broader protection for children and young people on all video-sharing platforms.
- **Exemptions to Age Assurance:** Implement a practical approach where age verification is only exempt for services that are highly unlikely to attract children, such as pension services or hardware suppliers.
- **Define 'Pornography':** The Code should include a clear definition of "pornography," covering both commercially produced and self-generated sexually explicit material.
- **Inclusion of Alcohol Advertising Restrictions:** The Code should align with public health laws, restricting alcohol advertising in locations where children are likely to be present, rather than just limiting advertising aimed specifically at children.

### Parental and other Restrictions:

- **Extend Protections to Existing Users:** Mandate that VSPS providers implement parental control systems not only for new users but also for existing users. This would ensure that children receive the same level of protection.
- **Include Privacy-by-Design Measures:** Require VSPS providers to implement privacy-by-design and safety-by-design measures for all users under 18 years, beyond just parental controls, to ensure a safer online experience regardless of parental oversight.
- **Strengthen Age Assurance Mechanisms:** Implement robust age assurance and verification methods to accurately identify and protect users who are under 18 years, ensuring that they are granted the appropriate protections from the outset.
- **Expand Parental Control Functionality:** Enhance the functionality of parental controls to allow for more granular control over content types, communication capabilities, and time management. The Code should require parental controls that allow parents to customise protections based on their child's age or developmental stage.

- **Address the 16–18 Age Group:** Introduce specific protections and safeguarding measures for users aged 16–18 years. This should include content moderation, privacy settings, and other safety features that address the continued, and in some ways the unique risks faced by older teens.
- **Mandate Transparency in Service Design:** Require VSPS providers to be transparent about their service design, including any inherent risks, and make safety-by-design a legal requirement rather than relying solely on parental controls and other reactive measures.
- **Develop a Continuous Evaluation Framework:** Require platforms to ensure that parental controls, privacy features, and safety mechanisms are regularly reviewed and updated based on emerging risks and technologies, providing an adaptive framework that grows with the needs of young users.

### Suspension of accounts:

- **Strengthen Child-Specific Remedial Mechanisms:** Implement child-specific remedial mechanisms that prioritise swift action to halt ongoing and future damage when a child is involved. This aligns with the UNCRC and the European Convention on Human Rights.
- **Mandate Immediate Removal of Harmful Content:** Require AVMS providers to immediately remove restricted or harmful content that involves or affects a child. The removal should be either permanent or interim, depending on the nature of the content, as soon as the provider becomes aware of it.
- **Recognise Single Serious Infringements:** Include a provision requiring immediate action from VSPS providers in response to single serious infringements that risk causing harm to a child. This would better align with the goal of protecting minors from content that may impair their development.
- **Child-Specific Focus in Responding to Restricted Content:** The Code should obligate providers to have particular regard when an infringement involves or impacts a child recognising the special obligations owed to child users.
- **Incorporate Child-Centred Safety Mechanisms:** Adopt practical, child-centred safety mechanisms, such as those outlined in the 5Rights Child Online Safety Toolkit, to ensure that reports of complaints involving children are monitored, evaluated, and swiftly addressed.
- **Ensure Access to Effective Remedies:** Guarantee that children who have had their rights violated by AVMS platform have access to effective remedies.
- **Enhance Provider Accountability for Child Protection:** Require that VSPS providers be held accountable for any failure to protect children, ensuring that their actions, or lack thereof, align with child protection obligations under the relevant legal frameworks

### Reporting and Flagging:

- **Mandate Age-Appropriate Reporting Mechanisms:** Require that VSPS providers establish and operate reporting and flagging mechanisms that are specifically designed to be age-appropriate, catering to the needs and comprehension levels of children and young people.
- **Ensure Prominence of Reporting Tools:** Obligate providers to make reporting and flagging mechanisms highly visible and easily accessible, particularly for younger users, ensuring that they can quickly and intuitively access these tools when needed.
- **Require Obligations for Reporting Illegal Content:** Require providers to establish and operate reporting mechanisms for all illegal content, not just content that falls within the restricted video content definition, with special emphasis on child protection.
- **Integrate Safeguards into Reporting Processes:** Include safeguards within the reporting and flagging processes that specifically account for the vulnerability of children and young people, ensuring that once content is reported, swift and protective action is required to be taken by AVMS providers.
- **Establish Child-Specific Support Following Reports:** Require providers to offer child-specific guidance and support after a report or flag has been made, ensuring that children and young

people understand the process, feel supported, and are aware of the next steps. Further, that VSPS are obligated to sign-post child and young users to specialist support services.

### Complaints and Enforcement:

- **Require Complaints Procedures be Age-Appropriate and Accessible:** Amend the Code to require that complaints procedures on video-sharing platforms be age-appropriate and accessible to child users, and those with disabilities.
- **Require the Prioritisation of Complaint made by or Involving Children:** Mandate that complaints involving children, or made by children, are prioritised and resolved within a specified timeframe.

### Include Recommender Systems:

- **Require the Code to Regulate Recommender Systems of Child Users:** Ensure the Code explicitly includes regulations on recommender systems for child users (those under 18 years). This should include provisions to mitigate risks such as exposure to harmful content, excessive screen time, and the creation of harmful content ‘rabbit holes’.
- **Mandate Child-Specific Protections Related to Recommender Systems:** The Code should require providers implement a ‘disable-by-default’ setting for personalised recommendations for users under 18 years, with the ability to enable these features only when it is age-appropriate and/or subject to parental/guardian.
- **Prohibit Profiling of Children and young People:** Prohibit the use of recommender systems that rely on profiling of children and young people.
- **Use the Code to Support the Implementation of the DSA:** Ensure that the Code aligns with the Digital Services Act (DSA) and the Audiovisual Media Services (AVMS) Directive by including protections against the risks posed by recommender systems, particularly regarding content delivery and exposure to harmful material.
- **Enhance Transparency and Accountability:** Mandate that service providers implement transparent decision-making processes for recommender systems, clearly communicating how content is delivered to children and young people and how harmful content is moderated or prevented.
- **Ensure Swift Intervention for Harmful Recommender Content:** The Code should require providers to take immediate action when recommender systems expose children to harmful content, prioritising swift removal and mitigation measures to protect their well-being.

### Illegal Content Harmful to Children:

- **Include Offence-Specific Harms in the Code:** The Code should include offence-specific harms, particularly those involving children, such as sexual grooming, child sexual abuse, trafficking, and the sharing of intimate images. This will better align the Code with Irish law and with the obligations under Article 28b(1) of the AVMS Directive. This will ensure that online platforms are explicitly required to address illegal content specific to Irish law, reinforcing child safety.
- **Promote Consistency Between the DSA and AVMS Directive:** Ensure that the Code is consistent with both the Digital Services Act (DSA) and the AVMS Directive, recognising that these pieces of legislation are interlocking and mutually reinforcing in enhancing online safety, particularly for children.
- **Enhance Reporting Mechanisms for Child-Specific Harms:** The Code should require platforms to implement robust, transparent, and user-friendly reporting mechanisms specifically for child-related harms, including illegal content such as child sexual abuse material and online grooming. In addition, VSPS should be obligated to sign-post child and young users to specialist support services where they report such content.



# 1. Introduction

The Children's Rights Alliance unites over 150 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 this opportunity to make a submission on the revised Online Safety Code ('the draft Code') published by Coimisiún na Meán ('the Coimisiún'), May 2024.<sup>1</sup> This response builds on our previous submissions to the Coimisiún in September 2023<sup>2</sup> and January 2024<sup>3</sup> in response to the 'call for input in the development of the Online Safety Code',<sup>4</sup> and the first draft Online Safety Code for video-sharing platform services,<sup>5</sup> respectively. This submission is informed by a consultation that was coordinated and run by the Children's Rights Alliance with our members in August 2024.

Incorporating a human rights approach into the Online Safety Code is essential to ensuring the protection of children in the digital age. The United Nations Convention on the Rights of the Child ("UNCRC") requires that every child has the right to privacy, freedom of expression, and protection from harmful content, which must be upheld in online environments.<sup>6</sup> Further elaborating on these rights, the UN Committee on the Rights of the Child's General Comment No. 25 on children's rights in relation to the digital environment emphasises that States must 'ensure that children's rights are respected, protected and fulfilled in the digital environment'.<sup>7</sup> This underscores the need for online safety policies and laws that not only prevent harm but also actively promote children's rights, balancing protective measures with the empowerment of children to fully engage in the digital world.

It has been well documented that children and young people in Ireland face numerous harms online, including exposure to inappropriate content,<sup>8</sup> cyberbullying,<sup>9</sup> privacy violations,<sup>10</sup> and online

---

<sup>1</sup> Coimisiún na Meán published revised (draft) Online Safety Code [May 2024](#)

<sup>2</sup> Submission to Coimisiún na Meán on Developing Ireland's First Binding Online Safety Code for Video-Sharing Platform Services - Children's Rights Alliance ([childrensrights.ie](http://childrensrights.ie)) [September 2023](#).

<sup>3</sup> Submission to Coimisiún na Meán on Developing Ireland's First Binding Online Safety Code for Video-Sharing Platform Services - Children's Rights Alliance ([childrensrights.ie](http://childrensrights.ie)) [January 2024](#)

<sup>4</sup> Coimisiún na Meán seeks views for developing Ireland's First binding Online Safety Code [July 2023](#)

<sup>5</sup> Coimisiún na Meán Consultation Document: Online Safety [December 2023](#)

<sup>6</sup> UN General Assembly, *Convention on the Rights of the Child* (adopted 20 November 1989, entered into force 2 September 1990), Article 16

<sup>7</sup> UN Committee on the Rights of the Child, General Comment No. 25, para. 4

<sup>8</sup> A study conducted by the Central Statistics Office (CSO) revealed that a significant number of children encounter harmful content online, including violence and pornography. The report highlighted that 23% of children aged 9-17 had seen sexual images in the past year, which can have detrimental effects on their mental and emotional well-being Central Statistics Office, 'Information Society Statistics – Households 2020' (CSO, 2020) <https://www.cso.ie/en/releasesandpublications/ep/p-iss/hh/informationstatistics-households2020/> accessed 22 July 2024.

<sup>9</sup> A meta-analysis of 39 published cyberbullying studies by Foody *et al* found a cybervictimisation rate of 13.7% for primary and 9.6% for post-primary students see M Foody, M Samara and J O'Higgins Norman, 'Bullying and Cyberbullying Studies in Ireland: A Meta-Analytical Review' (2017) 43 *Aggression and Violent Behaviour* 1. Research has demonstrated a significant link between bullying experiences in childhood and adolescence and the subsequent social and emotional development of those involved. For example, exposure to peer victimisation has been linked to anxiety, depression, low self-esteem, psychosis, and even suicide across all age groups Wolke, D., Copeland, W. E., Angold, A., & Costello, E. J. (2013). Impact of bullying in childhood on adult health, crime, and social outcomes. *Psychological Science*, 24, 1958–1970. <https://doi.org/10.1177/0956797613481608>.

<sup>10</sup> Privacy violations pose a serious risk to children online, with their personal information being exploited for commercial purposes or identity theft. In Ireland, CyberSafeKids (2022-2023) found that just 22% of 8 year olds but 59% of 16 year olds stated that they had private

grooming.<sup>11</sup> The prevalence of internet use by children and young people is significant, with a substantial number engaging with video-sharing platforms. According to the Central Statistics Office, 91 per cent of Irish children aged 8-12 use the internet, with 70 per cent accessing video-sharing platform services ('VSPS') regularly.<sup>12</sup> A VSPS, while offering educational and entertainment opportunities, also exposes young users to potential risks, including harmful content and cyberbullying. Research by the National Anti-Bullying Research and Resource Centre found that 40 per cent of Irish children have experienced cyberbullying.<sup>13</sup> There is also increasing evidence of pornography's role in shaping and fuelling violence against women and girls.<sup>14</sup> Additionally, the Former Special Rapporteur on Child Protection reported concerns about online grooming and exploitation facilitated by these platforms.<sup>15</sup>

We greatly welcome the publication of the draft Code. The work of the Coimisiún in this area is of critical importance in safeguarding the rights of children and young people in these ever-changing digital environments, and in working towards ensuring safer online experiences for everyone. However, we remain concerned that the draft Code does not sufficiently protect the rights of children and young people. In particular, the Alliance takes the view that the Coimisiún has not fully met its obligation under Article 28b(1) of Directive (EU) 2018/1808 in that it:

shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect: (a) minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1).

There is a tension between the permissive language of s.139K(2) Broadcasting Act (amended) and the mandatory language in Article 28b(1). The former states that a code 'may' make provision 'with a view' to ensuring 'that service providers take any other measures that are appropriate to provide the protections set out in Article 28b(1)' of the Directive. However, Article 28b(1) stipulates that 'Member States shall ensure that video-sharing platform providers under their jurisdiction 'take appropriate measures to protect minors from content which may impair their physical, mental or moral development in accordance with Article 6a(1)'. As such, the current draft Code falls short of fulfilling the Coimisiún's obligation to have 'regard to the safety of children in performing its functions'<sup>16</sup> and the 'particular commitment owed to the safety of children'.<sup>17</sup>

While the draft Code contains a general obligation in Part A to, 'as appropriate, establish and operate age verification systems with respect to content that may impair the physical, mental, or moral development of minors',<sup>18</sup> such content is now left largely undefined and the obligation a general, not child-specific one.

---

accounts. 32% of 8 year olds and 23% of 9 year olds were unsure of their privacy settings that on social media platforms, making them particularly vulnerable to data breaches. This lack of awareness often leads to oversharing personal information, which can be misused by malicious actors. A study by the European Commission (2020) on data protection practices found that many children do not fully understand the implications of sharing personal data online. This highlights the need for better education on digital literacy and privacy protection.

<sup>11</sup> National Children's Advocacy Center. (2024). The Online Manipulation (Grooming) of Victims of Sexual Abuse: A bibliography. Huntsville, AL: Author.; Wefers, S., Dieseth, T., George, E., Øverland, I., Jolapara, J., McAree, C., & Findlater, D. (2024). Understanding and deterring online child grooming: A qualitative study. *Sexual Offending: Theory, Research, and Prevention*, 19(1), 1-27. <https://doi.org/10.5964/sotrap.13147>;

<sup>12</sup> Central Statistics Office, 'Information Society Statistics – Households 2020' (CSO, 2020) <https://www.cso.ie/en/releasesandpublications/ep/p-iss/h/information-society-statistics-households2020/> accessed 23 July 2024.

<sup>13</sup> M Foody, M Samara and J O'Higgins Norman, 'Bullying and Cyberbullying Studies in Ireland: A Meta-Analytical Review' (2017) 43 *Aggression and Violent Behaviour* 1

<sup>14</sup> UK Government Equalities Office (GEO), 2020, The relationship between pornography use and harmful sexual attitudes and behaviours <https://www.gov.uk/government/publications/the-relationship-between-pornography-use-and-harmful-sexual-behaviours>; Children's Commissioner for England, 2023, "'A lot of it is actually just abuse": Young people and pornography', <https://assets.childrenscommissioner.gov.uk/wpuploads/2023/01/cc-pornography-and-young-people-information-sheet.pdf>;

<sup>15</sup> G Shannon, 'Report of the Special Rapporteur on Child Protection' (DCEDIY, 2019) <https://www.gov.ie/en/publication/06ab1d-report-of-the-special-rapporteur-on-child-protection-2019/> accessed 31 July 2024.

<sup>16</sup> 2009 Act, s.7(4)(a).

<sup>17</sup> 2009 Act, s.7(2)(b).

<sup>18</sup> Para 10.6(f) Online Safety Code [May 2024](#)



What previously constituted ‘regulated content harmful to children’ in the first draft of the Code included age-inappropriate content such as pornography, and content depicting gross and gratuitous violence. It also included dangerous challenges and covered a range of content that might pose a risk to the life, physical health, mental health and/or safety of a child: cyber-bullying, encouraging eating or feeding disorders, encouragement of self-harm or suicide, and information about methods of self-harm or suicide’. The terms ‘regulated content harmful to children’ and ‘illegal content harmful to children’ have now been subsumed within the definition of ‘restricted content’. While we welcome the expansion to better protect everyone online, we are concerned that the required responses, where the content involves a child are too limited and not child-specific enough.<sup>19</sup> For example, there is no requirement that Video-Sharing Platform Service providers (VSPS providers) expedite complaints relating to, involving, or made by children and young people and no specific algorithmic safeguards to protect child users from this content. Instead, the primary responsibility continues to fall on children and young people using the service to understand the terms and conditions and, where breached, to lodge a complaint, and on their parent/caregivers to effectively manage the Parental Control mechanisms. Children and young people have a right to an effective remedy under the European Convention of Human Rights,<sup>20</sup> and a child-friendly remedy as outlined in the Council of Europe Guidelines on Child Friendly Justice,<sup>21</sup> and under the UN Committee on the Rights of the Child’s guidance.<sup>22</sup> This obligation should be better incorporated into the Code.

Other concerns raised throughout this submission include the almost complete removal of obligations in the Code pertaining to illegal content, the limited requirements for age-verification, no requirement that accounts of children be private-by-default and the absence of responsibilities owed by VSPS providers to safeguard children and young people from the harms associated with recommender systems. The degree to which VSPS providers are still permitted to set their own goals and standards, and by the lack of baselines and targets being set by the Coimisiún are yet further concerns.

In our view, the draft Code, as it stands, does not adequately reflect the obligations under the AVMS Directive and, as such, constitutes a missed opportunity to protect, promote, and fulfil the rights of children and young people in the digital world.

---

<sup>19</sup> “restricted video content” means:

- (a) video content by which a person bullies or humiliates another person,
- (b) video content by which a person promotes or encourages behaviour that characterises a feeding or eating disorder,
- (c) video content by which a person promotes or encourages self-harm or suicide, (to include video content which encourages behaviour prejudicial to the health or safety of children, including dangerous challenges).
- (d) video content by which a person makes available knowledge of methods of self-harm, or suicide (to include video content which encourages behaviour prejudicial to the health or safety of children, including dangerous challenges).

where in the case of points (a)-(d) such content meets the risk test as defined in this Code.

<sup>20</sup> European Convention of Human Rights Arts 6 and 13

<sup>21</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).

<sup>22</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), para 44

## 2. Legislative context

A European Parliament Report stated the ‘regulatory objective’ of the Revised Audio-Visual Media Services Directive (EU) 2018/1808<sup>23</sup> (‘the AVMS Directive’) is ‘to create as coherent a legal framework as possible for content requirements ... and to hold platform operators accountable’.<sup>24</sup> It further observed that the general intention is to ‘effectively extend the scope of protection against illegal and harmful content and the regulated advertising environment to new online services’ without creating disadvantages for European Union providers directly competing with global platform providers.<sup>25</sup> The amendment of the Broadcasting Act 2009 (‘the 2009 Act’) by the Online Safety and Media Regulation Act 2022 (‘the 2022 Act’) constitutes Ireland’s transposition of the AVMS Directive. Relatedly, the 2009 Act has since been amended by the Digital Services Act 2024<sup>26</sup> which gave effect to Regulation (EU) 2022/2065 of the European Parliament and of the Council,<sup>27</sup> also known as the EU Digital Services Act (‘the DSA’). Of particular relevance to this commentary is Part 11 of the 2022 Act, which inserted a new Part 8A, entitled ‘Online Safety’, into the 2009 Act.

Pursuant to s.139K of the 2009 Act, the Coimisiún may make codes, known as ‘online safety codes’, to be applied to ‘designated online services’.<sup>28</sup> A designated online service is a ‘relevant online service’ designated pursuant to s.139E. A ‘relevant online service’, under s.2, means a ‘video-sharing platform service’ in the jurisdiction or any other information society service, save for an on-demand media service. In making such a designation under s.139E, the Coimisiún ‘shall designate as a category of services... the video-sharing platform services the provider of which is under the jurisdiction of the State’.<sup>29</sup> Accordingly, the Coimisiún has no choice but to apply the Code to ‘video-sharing platform services’ where the provider is under Irish jurisdiction. A ‘video-sharing platform service’ is a service whose principal purpose, a principal purpose of a dissociable section of the service, or an essential functionality of the service, is devoted to ‘providing audiovisual programmes or user-generated videos... in order to inform, entertain or educate’.<sup>30</sup>

In addition to video-sharing platform services, the Commission may designate other ‘relevant online services’ where their provider is under Irish jurisdiction.<sup>31</sup> In doing so, the designation may be in relation to a particular named service or in relation to all services falling within a certain category of services.<sup>32</sup> To make such a designation, s.139E(3) requires the Commission to have regard in particular to, among other factors:

- (d) levels of availability of harmful online content on the service, or on services within the category,
- (e) levels of risk of exposure to harmful online content when using the service, or services within the category,
- (f) levels of risk of harm, and in particular harm to children, from the availability of harmful online content or exposure to it on the service, or on services within the category,
- (g) the rights of the provider of the service, or providers of services within the category, and
- (h) the rights of users of the service, or users of services within the category.

<sup>23</sup> Which amended the previous Directive 2010/13/EU.

<sup>24</sup> European Parliament (2023), Report on the implementation of the revised Audiovisual Media Services Directive [https://www.europarl.europa.eu/doceo/document/A-9-2023-0139\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2023-0139_EN.html).

<sup>25</sup> *ibid.*

<sup>26</sup> Digital Services Act 2024 <https://www.irishstatutebook.ie/eli/2024/act/2/enacted/en/html>

<sup>27</sup> 19 October 2022, OJ L277, 27.10.2022

<sup>28</sup> A designated online service is one so designated under s.139E which permits, in circular fashion, the Coimisiún to ‘designate a relevant online service as a service to which online safety codes may be applied’. A ‘relevant online service’ means a ‘video-sharing platform service’ in the jurisdiction or any other information society service, save for an on-demand media service. It shall ‘designate as a named service under section 139E any relevant online service that appears to the Commission to be a video-sharing platform service the provider of which is under the jurisdiction of the State’. 2009 Act, s.2. 2009 Act, s.139E(1).

<sup>29</sup> 2009 Act, s.139G(1).

<sup>30</sup> 2009 Act, s.2.

<sup>31</sup> 2009 Act, s.139E(1).

<sup>32</sup> 2009 Act, s.139E(2).

These considerations are largely reflected *verbatim* in s.139L(3) which provides that, before making or revoking a determination that an online safety code is to apply to a designated online service or a designated category of services, the Coimisiún shall have regard in particular to listed factors.

Therefore, *the very designation* of a service under s.139E suggests some degree of availability of, and risk of exposure to, harmful online content for users, as well as a degree of risk of harm to children from the availability of, and exposure to, the said content. This means the starting point for an analysis of an online safety code is that a recognition of risk of harm to children is *built into* the framework. The Alliance does not consider that the Code as presently drafted takes due account of this fact, adequately or at all, as outlined in subsequent sections of this submission.

On 16 January 2024 the Commission published its statutory register of designated online services. The list of named video-sharing platform services is comprised of Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X, Pinterest, Tumblr, and Reddit.<sup>33</sup>

---

<sup>33</sup> Comisiún na Meán, 'Register of designated relevant online services pursuant to S139J of the Broadcasting Act 2009 as amended' (16 January 2024) <https://www.cnam.ie/designation-notices/>.

### 3. Age verification/assurance limited to adult-only content

#### Age Assurance

There is no obligation in the draft Code to restrict children's access to most VSP services through age verification, even though it notes that 'there is potential for harm when underage users are able to open accounts on video-sharing platforms.'<sup>34</sup>

In addition, the draft Code contains a general requirement that VSPS providers implement age verification systems for users accessing content that could harm the physical, mental, or moral development of minors.<sup>35</sup> This requirement intends to align the Code with the intent of Article 28b(1) of the AVMS Directive. However, the only 'more specific measure' to effect age assurance - as opposed to the general obligation in Part A<sup>36</sup> - deals with age assurance as it relates to platforms devoted to 'adult-only content'.<sup>37</sup>

In addition, that approach, where age assurance is the exception, can only result in a situation where few VSPS providers will require age verification, including those providers offering social media accounts. It is our view that this approach does not adequately safeguard and protect the rights of children and young people online. If An Coimisiún recognises that a potential for harm exists when underage users are able to open and use accounts on video-sharing platforms, restrictions, by way of age verification seems like a practical and necessary solution.

Age verification should not be viewed as simply restricting children and young people from digital world, or parts thereof. Age verifications, when working at their best invite children into a safer digital world, offering greater privacy, freedom from commercial pressures, protection from harmful content, and fostering the development of new services that recognise children as a key user group.<sup>38</sup>

In an approach which also recognises the potential for harm for children and young people, the 5Rights Foundation reverses the presumption of exceptional use of age assurance. Instead, they propose that:

'given the vast array of digital technologies and the millions of services available, it is more practical to identify scenarios where age assurance is *not* required rather than trying to pinpoint every product or service that does. For instance, age verification is unnecessary for services unlikely to attract children, such as pension services, hardware suppliers, or estate agents. Likewise, products or services with child-centred design, mixed-audience services, those requiring unique user identification, and certain educational or news resources may also be exempt.<sup>39</sup> Importantly, it is only after a thorough review, which ensures that harmful content is effectively filtered that sites are deemed safe should be exempt from the age verification requirement.<sup>40</sup>

---

<sup>34</sup> Consultation Document, p. 17.

<sup>35</sup> Para. 10.6(f) Online Safety Code [May 2024. The Code states: A video-sharing platform service provider shall establish and operate age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors.](#)

<sup>36</sup> Coimisiún na Meán, 'Response to Consultation: Online Safety Code' (27 May 2024), p. 16.

<sup>37</sup> Para. 12.11 Online Safety Code [May 2024](#)

<sup>38</sup> 5Rights Foundation, 'But How Do They Know It Is A Child?' (2023), p.9  
[https://5rightsfoundation.com/uploads/But\\_How\\_Do\\_They\\_Know\\_It\\_is\\_a\\_Child.pdf](https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf)

<sup>39</sup> 5Rights Foundation, 'But How Do They Know It Is A Child?' (2023), p.15-16  
[https://5rightsfoundation.com/uploads/But\\_How\\_Do\\_They\\_Know\\_It\\_is\\_a\\_Child.pdf](https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf)

<sup>40</sup> 5Rights Foundation, 'But How Do They Know It Is A Child?' (2023), p.15-16  
[https://5rightsfoundation.com/uploads/But\\_How\\_Do\\_They\\_Know\\_It\\_is\\_a\\_Child.pdf](https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf)

We believe this is a reasonable approach and one that should be included in the Code.

How children and young people experience content will be different from how adults experience content. What is considered harmful to a child may not be so to an adult. There is a real risk that without a comprehensive requirement for age verification, other ameliorative measures, such as parental controls for users under the age of 16,<sup>41</sup> restrictions on content that is harmful to children, or restricting content that should not 'normally be seen by children', cannot be effectively implemented, thus limiting their utility in protecting children and young people online.

Article 28b(1) of the AVMS Directive requires the Coimisiún to protect children against content 'which may impair their physical, mental or moral development'. The word 'may' sets down a much lower threshold than that appearing in the draft Code. If there is no requirement that a provider have a mechanism for determining whether a person is a child there is no way this assessment can accurately be undertaken

### Effective age assurance for 'adult-only' video content

The draft Code requires that a video-sharing platform service provider which does not prohibit 'the uploading or sharing of adult-only video content... shall implement effective age assurance measures as defined in this Code'.<sup>42</sup>

An 'age assurance measure' is defined as 'a process used to restrict access to a service or to particular features or content of a service that involves estimating or verifying a user's age'.<sup>43</sup> Save for a statement that 'self-declaration of age by users does not constitute an effective measure', there is no guidance in the draft Code as to what an effective 'age assurance measure' might be.

The draft Code defines adult-only content as 'video content consisting of pornography' and 'video content consisting of realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty'.<sup>44</sup> It does not include commercial services relating to alcohol as adult-only content, despite clearly recognising its risks.

Part B of the Code requires VSPS providers who, in their terms and conditions, permit the uploading or sharing of adult-only content to implement 'effective age assurance measures'<sup>45</sup> and where adult-only content is permitted that such content be rated as 'as not suitable for children' by the uploader.<sup>46</sup> There is also a requirement 'precluding the use by children ...and an obligation that adult users ensure that their accounts on the service are not used by children'.<sup>47</sup> The combined aim of these measures is intended to ensure that such video content 'cannot ordinarily be seen by children'.<sup>48</sup> However, without a quantifiable benchmark for what will be considered 'effective' we are concerned that this will not be sufficient to protect children from this content. Moreover, children are increasingly being exposed to harmful content, including pornography and violence, on social media and other online platforms.<sup>49</sup> While the content may, in the strictest sense be 'legal',

---

<sup>41</sup> The Code specifies 16 years. However, we recommend that this be 18.

<sup>42</sup> Para. 12.11 Online Safety Code [May 2024](#)

<sup>43</sup> Para 12 Online Safety Code [May 2024](#)

<sup>44</sup> Para 11 Online Safety Code [May 2024](#)

<sup>45</sup> Para 12.11 Online Safety Code [May 2024](#)

<sup>46</sup> Para 12.12 Online Safety Code [May 2024](#)

<sup>47</sup> Para 12.4 Online Safety Code [May 2024](#)

<sup>48</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024,

<sup>49</sup> Studies have revealed that younger children, even under the age of 10, are at risk of encountering sexual material online, often through coercion and manipulation by online predators. The Internet Watch Foundation reported a significant rise in child sexual abuse imagery in 2023, with many cases involving children as young as primary school age being coerced into creating explicit content, which is then widely shared across criminal networks. Internet Watch Foundation, 'Under 10s Groomed Online "Like Never Before" as Hotline Discovers Record Amount of Child Sexual Abuse' (IWF, 25 April 2024) <https://www.iwf.org.uk/news-media/news/under-10s-groomed-online-like-never-before-as-hotline-discovers-record-amount-of-child-sexual-abuse>; NSPCC, 'Children's Experiences of Legal but Harmful Content Online' (NSPCC, February 2022) <https://learning.nspcc.org.uk/research-resources/2022/helplines-insight-briefing-legal-but-harmful-content>



exposing a child to sexualised imagery is not.<sup>50</sup> We are also concerned at the continued failure to define pornography in a comprehensive way, or to include.

## Pornography

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>51</sup> but some children accessing it by the time they are 9 years old.<sup>52</sup> That Report also found that children ‘often stumble accidentally across pornography online’<sup>53</sup> and X (formerly Twitter) was the platform where the greatest number of children had seen pornography.<sup>54</sup> Such content not only impacts the physical, mental, and moral development of children, but can also impede their social development.

We recommend that the Code should include a non-exhaustive definition of pornography and this must include sexually explicit material that has been self-generated, rather than being restricted to pornography which is generated for commercial interests. It must also be borne in mind that pornography is also carried across many digital platforms, not just those that present as adult-only content platforms. As noted above, it is for that reason that we believe that age verification should be the norm AVMS platforms, especially for social media account creation and use, and not the exception.

## Highly effective age assurance

The powers and functions of the Coimisiún include that it ‘shall endeavour to ensure... that the interests of the public, including the interests of children, are protected, with particular commitment to the safety of children’.<sup>55</sup> In order to fulfil this function, the draft Code must specify that highly effective age assurance is necessary to ensure that platforms implement measurable standards for protecting children online. Defining, and quantifying these standards can prevent a ‘race to the bottom’ where less rigorous platforms compromise child safety, ensuring that Ireland’s online environment remains secure for minors.<sup>56</sup>

## Commercial AV content on alcohol

The Code does not define the advertising, marketing, selling, or arranging of alcohol and or the advertising of alcohol as ‘adult-only content’. It specifically states that a ‘video-sharing platform service provider shall not be restricted from marketing, selling or arranging, and (in the case of audiovisual commercial communications not marketed, sold, or arranged by them) shall not be required to preclude audiovisual commercial communications for alcohol provided that such content cannot normally be seen by children’.<sup>57</sup> The measures required to fulfil this obligation are ‘content rating, age assurance and parental controls’.<sup>58</sup> While alcohol advertising is included in the definition of ‘audiovisual commercial communications harmful to children’ this is limited to ‘audiovisual commercial communications for alcohol aimed specifically at children’. This only restricts alcohol advertising that is ‘aimed specifically at children’ – which appears to fall far shorter than the prohibitions set out in the Public Health (Alcohol) Act 2018 which, among other things, prohibits alcohol advertising in locations where children are likely to be present, such as near schools, playgrounds, and public parks.

---

<sup>50</sup> 2017 Act

<sup>51</sup> Children’s Commissioner for England, ‘A lot of it is actually just abuse’ Young people and pornography’ January 2023, 6 -8.

<sup>52</sup> Children’s Commissioner for England, ‘A lot of it is actually just abuse’ Young people and pornography’ January 2023, 6 -8.

<sup>53</sup> Children’s Commissioner for England, ‘A lot of it is actually just abuse’ Young people and pornography’ January 2023, 6 -8.

<sup>54</sup> Children’s Commissioner for England, ‘A lot of it is actually just abuse’ Young people and pornography’ January 2023, 6 -8. 2009 Act, s.7(2)(b).

<sup>55</sup> ‘Highly Effective Age Assurance Poorly Defined in Ofcom Consult, Says AVPA’ (Biometric Update, 21 August 2024)

<https://www.biometricupdate.com/202407/highly-effective-age-assurance-poorly-defined-in-ofcom-consult-says-avpa>

<sup>57</sup> Para 13.14 Online Safety Code [May 2024](#)

<sup>58</sup> Para 13.14 Online Safety Code [May 2024](#)

## Recommendations

- **Effective Age Assurance Measures:** The Code should provide for a clear obligation on what constitutes an effective age assurance measure to include a quantifiable benchmark.
- **Comprehensive Age Assurance Implementation:** The Code should extend age assurance requirements beyond adult-only content to ensure broader protection for children and young people on all video-sharing platforms.
- **Exemptions to Age Assurance:** Implement a practical approach where age verification is only exempt for services that are highly unlikely to attract children, such as pension services or hardware suppliers.
- **Define 'Pornography':** The Code should include a clear definition of "pornography," covering both commercially produced and self-generated sexually explicit material.
- **Inclusion of Alcohol Advertising Restrictions:** The Code should align with public health laws, restricting alcohol advertising in locations where children are likely to be present, rather than just limiting advertising aimed specifically at children.

## 4. Parental and other restrictions

As per part 14 of the draft Code, VSPS providers which permit users under the age of 16 to access their service are required to operate parental control systems that, at a minimum, have the functionality to enable the parent or guardian to restrict a child from viewing video content uploaded or shared by users that are unknown to the child; to restrict viewing of video content uploaded or shared by the child by users that are unknown to the child; restrict a child from viewing video content or audiovisual commercial communications based on language terms contained in the description of the video or commercial communication or based on metadata about the video or commercial communication; and set time limits in respect of viewing of video content.<sup>59</sup> The Code limits this requirement as an option to new users on account sign-up for the service.<sup>60</sup> As this requirement will not apply to existing users, this will leave those users who have already signed up deprived of this limited protection. At a minimum, the Code must provide the same protection to children, whether they are new or existing users.

It is welcome to see that the Coimisiún acknowledges that parental controls are but one measure for protecting children online. This is clear as they are cited among the list of ameliorating measures throughout the Code, age assurance, content rating, and reporting and flagging. However, these measures '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>61</sup> There is also a question as to what protections measures are available for young people aged 16–18. While the Code recognises children as those who are under 18 years, there does not appear to be any requirements placed on VSPS providers to safeguard the rights of this cohort of users, other than the general obligation in section 10.6, which remains a general and non-specific obligation.

The Code only requires that Parental Controls be made available, where a VSPS provider permits users under 16.<sup>62</sup> There is no requirement that providers are required to provide any safety or privacy-by-design measures for children. The only requirement in the Code is that VSPS providers make parental controls available where they permit users who are under 16 years. Without requiring age verification/assurance for account creation and use there is simply no way to guarantee that a user has reached the minimum age for use, or that they are not afforded the, albeit limited protections offered by parental controls.

### Recommendations

- **Extend Protections to Existing Users:** Mandate that VSPS providers implement parental control systems not only for new users but also for existing users. This would ensure that children receive the same level of protection.
- **Include Privacy-by-Design Measures:** Require VSPS providers to implement privacy-by-design and safety-by-design measures for all users under 18, beyond just parental controls, to ensure a safer online experience regardless of parental oversight.
- **Strengthen Age Assurance Mechanisms:** Implement robust age assurance and verification methods to accurately identify and protect users who are under 18, ensuring that they are granted the appropriate protections from the outset.
- **Expand Parental Control Functionality:** Enhance the functionality of parental controls to allow for more granular control over content types, communication capabilities, and time

---

<sup>59</sup> Para 14 Online Safety Code [May 2024](#)

<sup>60</sup> Para 14.15 Online Safety Code [May 2024](#)

<sup>61</sup> 5Rights Foundation, '5Rights Framework for Children's Rights Online' (Ofcom, 2021) [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>62</sup> Para 14.1 Online Safety Code [May 2024](#)

management. The Code should require parental controls that allow parents to customise protections based on their child's age or developmental stage.

- **Address the 16–18 Age Group:** Introduce specific protections and safeguarding measures for users aged 16–18. This should include content moderation, privacy settings, and other safety features that address the continued, and in some ways the unique risks faced by older teens.
- **Mandate Transparency in Service Design:** Require VSPS providers to be transparent about their service design, including any inherent risks, and make safety-by-design a binding requirement rather than relying solely on parental controls and other reactive measures.
- **Develop a Continuous Evaluation Framework:** Require platforms to ensure that parental controls, privacy features, and safety mechanisms are regularly reviewed and updated based on emerging risks and technologies, providing an adaptive framework that grows with the needs of young users.

## 5. Suspension of accounts

As the revised definitions of restricted content apply to all users, adult and child, there is an obligation in the Code that an AVMS provider have particular regard when an infringement involves or impacts on a child.<sup>63</sup> There is insufficient recognition of the special obligations owed to child and young users. Children and young people must have access to remedial mechanisms that 'take into account the vulnerability of children and the need to be swift to halt ongoing and future damage'.<sup>64</sup> The 5Rights Child Online Safety Toolkit provides practical examples of child-centred safety mechanisms, emphasising the importance of putting in place mechanisms that allow for reports of complaints to be monitored and evaluated so that areas of concern can be swiftly identified and addressed.<sup>65</sup> This aligns with Article 16 of the UNCRC, which protects children's privacy and dignity, demanding that complaints processes respect these principles. It is vital to ensure that children and young people whose rights are not respected by the VSPS provider and who have exhausted all appropriate channels with the service or platform, have access to an effective remedy in line with their rights under the European Convention of Human Rights.<sup>66</sup>

We note that the obligation to terminate user accounts for infringements of terms and conditions has been removed in revised Code. Part B now requires VSPS providers to suspend, after prior warning and for a reasonable period, services to users who 'frequently' infringe the terms and conditions.<sup>67</sup> The Code does require AVMS providers to make provision for the immediate take down of restricted or harmful content that involves a child, relates to a child, or has been flagged by a child. The Code should require that a provider be required to immediately remove such content on either a permanent or interim basis as soon as the provider is aware of it. Moreover, section 12.9 should also include the obligation to protect children and young people under article 28b(1)(a) of the AVMS Directive.

Failing to include a provision requiring VSPS providers to act where there is a single serious infringement which causes or risks causing harm to a child is not, in our view, an 'appropriate measure to protect minors' from content which may impair their physical, mental or moral development' in line with article 28b(1)(a) of the AVMS Directive.

In addition to the suspension of accounts that frequently breach the terms of service, the Alliance is strongly of the view that the Code must also provide for the immediate removal of single serious infringements that pose harm to or involve harm to children and explicitly recognised this duty in the Code.

### Recommendations

- **Strengthen Child-Specific Remedial Mechanisms:** Implement child-specific remedial mechanisms that prioritise swift action to halt ongoing and future damage when a child is involved. This aligns with the UNCRC and the European Convention on Human Rights.

---

<sup>63</sup> The first draft of the Code defined a number of different forms of harmful content. Namely: Audiovisual commercial communications harmful to children.

- Audiovisual commercial communications harmful to the general public.
- Illegal content harmful to children.
- Illegal content harmful to the general public.
- Regulated content harmful to children.
- Regulated content harmful to the general public.

<sup>64</sup> UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (2 March 2021) UN Doc CRC/C/GC/25, para 46

<sup>65</sup> 5Rights Foundation, *Child Online Safety Toolkit* (5Rights Foundation 2022) 42 <https://childonlinesafetytoolkit.org/wp-content/uploads/2022/05/5Rights-Child-Online-Safety-Toolkit-English.pdf>, p.29

<sup>66</sup> European Convention of Human Rights Arts 6 and 13

<sup>67</sup> Para 12.7 and 13.7 Online Safety Code [May 2024](#)



- **Mandate Immediate Removal of Harmful Content:** Require AVMS providers to immediately remove restricted or harmful content that involves or affects a child. The removal should be either permanent or interim, depending on the nature of the content, as soon as the provider becomes aware of it.
- **Recognise Single Serious Infringements:** Include a provision requiring immediate action from VSPS providers in response to single serious infringements that risk causing harm to a child. This would better align with the goal of protecting minors from content that may impair their development.
- **Child-Specific Focus in Responding to Restricted Content:** The Code should obligate providers to have particular regard when an infringement involves or impacts a child recognising the special obligations owed to child users.
- **Incorporate Child-Centred Safety Mechanisms:** Adopt practical, child-centred safety mechanisms, such as those outlined in the 5Rights Child Online Safety Toolkit, to ensure that reports of complaints involving children are monitored, evaluated, and swiftly addressed.
- **Ensure Access to Effective Remedies:** Guarantee that children who have had their rights violated by AVMS platform have access to effective remedies.
- **Enhance Provider Accountability for Child Protection:** Require that VSPS providers be held accountable for any failure to protect children, ensuring that their actions, or lack thereof, align with child protection obligations under the relevant legal frameworks

## 6. Reporting and flagging

Transparent mechanisms for reporting and flagging are essential. While the Code provides for an obligation that VSPS providers establish transparent and user-friendly mechanisms for users to report or flag content,<sup>68</sup> there is no obligation in the Code that these mechanisms be age-appropriate and prominent.<sup>69</sup>

Since the December 2023 draft Code, the scope of the Code has been narrowed to exclude offence-specific harms. The revised Code does *not* now require that providers establish and operate a reporting and flagging mechanism for content that is illegal, except for content that falls within the definition of restricted video content. As with the above analysis ('suspension of accounts'), the removal of requirements around illegal content, coupled with the expansion of restricted content to include both adults and children there is a danger that the Code fails to adequately recognise the special duty owed to the protection of children and young people. Without the Code requiring that providers operate an age-appropriate reporting and flagging system will further compound this issue.

The Code should include a requirement that providers establish and operate a reporting or flagging mechanism that is age-appropriate and designed to meet the needs of children and young people.

### Recommendations

- **Mandate Age-Appropriate Reporting Mechanisms:** Require that VSPS providers establish and operate reporting and flagging mechanisms that are specifically designed to be age-appropriate, catering to the needs and comprehension levels of children and young people.
- **Ensure Prominence of Reporting Tools:** Obligate providers to make reporting and flagging mechanisms highly visible and easily accessible, particularly for younger users, ensuring that they can quickly and intuitively access these tools when needed.
- **Require Obligations for Reporting Illegal Content:** Require providers to establish and operate reporting mechanisms for all illegal content, not just content that falls within the restricted video content definition, with special emphasis on child protection.
- **Integrate Safeguards into Reporting Processes:** Include safeguards within the reporting and flagging processes that specifically account for the vulnerability of children and young people, ensuring that once content is reported, swift and protective action is required to be taken by AVMS providers.
- **Establish Child-Specific Support Following Reports:** Require providers to offer child-specific guidance and support after a report or flag has been made, ensuring that children and young people understand the process, feel supported, and are aware of the next steps. Further, that VSPS are obligated to sign-post child and young users to specialist support services.

---

<sup>68</sup> Para 15 Online Safety Code [May 2024](#)

<sup>69</sup> Information Commissioner's Office, 'Age Appropriate Design: A Code of Practice for Online Services', p. 83-84

## 7. Complaints and enforcement

There is no obligation in the Code that the complaints procedures operated by a video-sharing platform be age-appropriate. Nor is there a requirement that complaints by children, or involving children be dealt with in a specified time. Instead, the Code requires that the platform ‘handle complaints in a diligent, timely and non-discriminatory, and effective manner’.<sup>70</sup> It is essential that the Code requires that providers operate a complaints mechanism that is not only transparent, but one that is age appropriate and accessible to child and young users. Complaints procedures should require platforms to have particular regard to complaints that are made by child users, or that involve children. Further, it is concerning that there is no explicit requirement that complaints procedures be accessible to persons with disabilities.

UNCRC includes specific obligations to ensure that children with disabilities enjoy their full range of human rights without discrimination. Article 23 of the Convention emphasises that children with disabilities have the right to a full and decent life, in conditions that ensure dignity, promote self-reliance, and facilitate the child's active participation in the community. States are required to recognise the special needs of disabled children and take appropriate measures to provide them with access to healthcare, education, rehabilitation services, and preparation for employment and recreation, in a manner conducive to their fullest possible social integration and individual development. This reflects a broader commitment to equality, ensuring that these children are supported to reach their potential while enjoying all rights granted to every child under the Convention.

It is vital to ensure that children and young people whose rights are not respected by platforms and who have tried to resolve the issue with the platform, have access to an effective remedy in line with their rights under the European Convention of Human Rights.<sup>71</sup> This should also align with the clear description of a child-friendly remedy outlined in the Council of Europe Guidelines<sup>72</sup> while also complying with the UN Committee on the Rights of the Child’s guidance.<sup>73</sup>

### Recommendations

- **Require Complaints Procedures be Age-Appropriate and Accessible:** Amend the Code to require that complaints procedures on video-sharing platforms be age-appropriate and accessible to child users, and those with disabilities.
- **Require the Prioritisation of Complaint made by or Involving Children:** Mandate that complaints involving children, or made by children, are prioritised and resolved within a specified timeframe.

---

<sup>70</sup> Para 16 Online Safety Code [May 2024](#)

<sup>71</sup> European Convention of Human Rights Arts 6 and 13

<sup>72</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).

<sup>73</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), para 44

## 8. Absence of recommender systems in the Code

Harm stemming from social media does not come from content alone, but also from the design of platforms.<sup>74</sup> Recommender systems, while designed to enhance user experience by tailoring content to individual preferences, can cause significant harm to children.<sup>75</sup> One of the primary concerns is the exposure to inappropriate or harmful content. Algorithms prioritise engagement and often push sensational or extreme content to maintain user attention.<sup>76</sup> As a result, children are being exposed to violent, sexual, or otherwise age-inappropriate material. This exposure can have detrimental effects on their psychological development and overall well-being, contributing to issues such as increased anxiety, fear, and desensitisation to violence.<sup>77</sup> Moreover, recommender systems can contribute to the development and reinforcement of harmful behaviours. For instance, algorithms that promote content related to body image can lead children towards materials that encourage eating disorders or unhealthy body standards. Similarly, children might encounter content that glamorises risky behaviours, self-harm, or substance abuse. The repetition of such content can normalise these behaviours, increasing the likelihood of children emulating them.<sup>78</sup> The persistence of such harmful content in children's digital environments underscores the need for stringent regulatory measures to mitigate these risks.

Privacy and data protection concerns are also prominent when it comes to children using platforms with recommender systems. These systems rely on extensive data collection, including personal preferences, browsing habits, and engagement metrics, to function effectively.<sup>79</sup> For children, this can mean invasive data practices that do not fully consider their right to privacy and protection from exploitation. Under the UNCRC, children have the right to privacy (Article 16) and the right to be protected from all forms of physical or mental violence, injury, abuse, neglect, and exploitation (Article 19). The lack of transparency and understanding about how their data is being used and the potential for misuse, including targeted advertising and behavioural profiling, poses significant risks.<sup>80</sup> It is imperative that platforms adopt stricter data protection measures for children, ensuring that their digital footprint does not lead to long-term adverse consequences.

It would appear that the Coimisiún had originally intended to include recommender systems in draft supplementary measures and guidance to the Code.<sup>81</sup> In the December 2023 draft Code, the Coimisiún published 'draft supplementary measures and guidance' which included a section on 'recommender system safety', and the statement that video-sharing platform service providers 'must ensure that the operation of recommender systems does not result in a user being exposed to content which, in aggregate, causes harm'. According to the Coimisiún in their response to the

---

<sup>74</sup> McGrath, C. (2023, September 29). What is online harm: And how do we define it? RTE. <https://www.rte.ie/brainstorm/2023/0929/1407929-online-harm-ireland-online-safety-and-media-regulation-act-eu-digital-services/>

<sup>75</sup> Social media algorithms significantly harm adolescents, particularly affecting mental health issues like body dissatisfaction, anxiety, and depression. Legal strategies to regulate these harms are more likely to succeed at the state level, with promising solutions including mandatory algorithm risk audits conducted by third parties to protect adolescent mental health see Amanda Raffoul et al, 'Adolescent Mental Health and Big Tech: Investigating Policy Avenues to Regulate Harmful Social Media Algorithms' (2023) 72 *Journal of Adolescent Health* S12 < <https://www.jahonline.org/action/showPdf?pii=S1054-139X%2822%2900828-X> >. Harms result from complex socio-technical systems involving algorithms, platform design, commercial interests, and social practices, not just algorithms alone. The article suggests governance interventions, emphasising the need for external oversight to address the increasing power of platforms alongside correcting algorithmic errors see Saurwein, Florian; Spencer-Smith, Charlotte (2021). Automated Trouble: The Role of Algorithmic Selection in Harms on Social Media Platforms. *Media and Communication*, 9(4):222-233.

<sup>76</sup> Dujancourt, E., & Garz, M. (2023). The effects of algorithmic content selection on user engagement with news on Twitter. *The Information Society*, 39(5), 263–281. <https://doi.org/10.1080/01972243.2023.2230471>

<sup>77</sup> Livingstone, S., and Helsper, E. (2006). "Does advertising literacy mediate the effects of advertising on children?" *Public Understanding of Science*, 15(3), 296-312

<sup>78</sup> Byrne, J., Kardefelt-Winther, D., Livingstone, S., and Stoilova, M. (2018). "Global Kids Online research synthesis, 2015-2016." UNICEF Office of Research - Innocenti

<sup>79</sup> Ishita Choudhary, 'The power of data: How recommendation engines are driving business growth',

<https://www.mindtheproduct.com/the-power-of-data-how-recommendation-engines-are-driving-business-growth/>

<sup>80</sup> Stoilova, M., Livingstone, S., and Nandagiri, R. (2020). "Children's data and privacy online: Growing up in a digital age." LSE Department of Media and Communications.

<sup>81</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024

Consultation on the draft Code, the implementation of requirements such as safety by design and online safety supports ‘merits further deliberation’. Accordingly, it had given the impression that such measures may be addressed through statutory guidance.<sup>82</sup> On the regulation of recommender systems the Coimisiún’s position appears somewhat different to that of safety-by-design and other protection measures in that they expressly acknowledge ‘that recommender systems can play a significant role in creating harm to minors’.<sup>83</sup> Not simply this, but it goes further by detailing *how* recommender feeds *should* be designed to prevent risk to children, specifically stating:

The Commission considers that to reduce this harm, recommender systems that create feeds of content for minors should be designed to avoid risks such as:

- creating feeds of content that are harmful in aggregate (including by creating a ‘rabbit-hole’ effect)
- encouraging minors to spend a harmful amount of time using the service
- amplifying harmful or age-inappropriate content
- recommending content based on profiling of minors, unless there are child-centred ways for users to configure their profiling options.<sup>84</sup>

In the response to the consultation, in May 2024 the Coimisiún expressly acknowledged that ‘recommender systems that are not so designed are likely to be unsafe for minors’.<sup>85</sup> Yet, despite this, the Coimisiún determined that recommender systems are more appropriately addressed under the DSA, and that it did not ‘propose to take further the possibility of a supplementary Online Safety Code at this time’.<sup>86</sup>

Beyond including recommender systems or supplementary measures and guidance associated with the Safety Codes, the actions proposed by the Coimisiún to address these systems are to continue supporting European Commission investigations into whether recommender systems are operating in compliance with the DSA; use its own supervisory powers, in cooperation with the European Commission as appropriate, to examine the compatibility of recommender systems with Article 28 of the DSA; and as a member of the European Board for Digital Services, to participate in the development of guidelines to be issued under Articles 28 and 35 of the Digital Services Act.<sup>87</sup>

The change in approach by the Coimisiún to now exclude reference to recommender systems appears to stem from submissions to the Coimisiún by TikTok and Meta, wherein it was argued that as the AVMS Directive made no ‘express reference to the regulation of’ recommender systems ‘it is unclear... the basis on which the draft Code is seeking to regulate the use of recommender systems’.<sup>88</sup> TikTok submitted that the inclusion of recommender systems within the Code would go ‘significantly further than, and is in conflict with, the DSA’, and that ‘the proposal runs the clear risk of creating inconsistent, parallel regulation of very similar subject matter’.<sup>89</sup>

The Alliance does not consider that there would be any such ‘conflict’ or ‘inconsistent, parallel regulation’ of recommender systems between the DSA and the Directive. Both apply in Ireland as EU law, and EU law cannot be in conflict with itself (if a conflict were to arise, this would require to be adjudicated by the Court of Justice of the EU). In fact, the European Commission has referred to the DSA and the AVMS Directive as constituting, among other pieces of EU law, ‘the EU legal and policy

---

<sup>82</sup>Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024, para. 4.2

<sup>83</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024, Para 4.2

<sup>84</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024, p.18

<sup>85</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024

<sup>86</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024, Para 4.2

<sup>87</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024, pp.18-19

<sup>88</sup> Coimisiún na Meán, Response to Consultation: Online Safety Code, Publication date: 27 May 2024, p.26

<sup>89</sup> Ref TikTok. Similarly, Meta submitted that “the Commission proposes to include in a future iteration of the Code a requirement for VSPS providers to implement a recommender system safety plan”. It said “the AVMSD is silent on such a measure, but it is addressed in the DSA”. It said “recommender systems standards are already harmonised by the DSA (see Articles 27 and 38 of the DSA). As such, and once again, this supplementary measure is not necessary in MPIL’s view and it is unclear what this additional proposal seeks to achieve.”



framework to ensure even more effective child online safety'.<sup>90</sup> Moreover, the Coimisiún itself has indicated its purpose as being to put in place 'the Online Safety Framework in Ireland', which is comprised of the 2022 Act which forms 'the basis for our draft Online Safety Code', the DSA, and the EU Terrorist Content Online Regulation.<sup>91</sup> The DSA and the Directive are interlocking and mutually reinforcing pieces of legislation designed to enhance online safety as a whole. That the 2022 Act (and the AVMS Directive) is considered 'the basis' for the online safety code does not mean other relevant matters cannot be incorporated, and should include recommender systems, which are indeed covered by the DSA.<sup>92</sup>

That the AVMS Directive did not expressly reference recommender systems is of little consequence, in the Alliance's view, as its principles seem rather clearly to include them. Section 139K of the 2009 Act, transposing the AVMS Directive, provides that the Coimisiún may make a code with a view to ensuring, among other things, that service providers take appropriate measures to minimise the availability of harmful online content and risks arising from the availability of and exposure to such content. This aim is broadly stated, and the minimisation of the 'exposure' to harmful online content seems directly linked to the recommender system in use. Section 139K(2)(c) requires the taking of appropriate measures to provide the protections set out in Article 28b(1)(a)–(c) of the AVMS Directive, which includes protecting 'minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1)'. Article 6a(1) obliges Member States to 'take appropriate measures to ensure' that media 'which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them'. The AVMS Directive and the 2009 Act oblige the Coimisiún to ensure that children will not normally see content which may impair their development: a primary way of accomplishing this *cannot but be* regulation of the recommender systems. The below legislative elements, read in unison, offer further support for this view:

- (i) the stipulation of appropriate measures to minimise the availability of, and protect services users from, harmful online content and risks arising from the availability of and exposure to such content;<sup>93</sup>
- (ii) that an online safety code may provide for standards, practices and measures which apply to service providers, particularly as regards 'the moderation of content' or 'how content is delivered';<sup>94</sup>
- (iii) that such a code may be drafted having regard to the desirability of services having transparent decision-making processes in relation to content delivery and content moderation;<sup>95</sup> and
- (iv) that a code may also be drafted having regard to the levels of risk of harm, and in particular harm to children, from the availability of harmful online content or exposure to it.<sup>96</sup>

There is therefore nothing within the 2009 Act, the AVMS Directive, nor the DSA to suggest that the Code cannot include recommender system protections. On the contrary, there are exceptionally good reasons to suggest that given the specific obligations owed to children, this Code and future

---

<sup>90</sup> European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Decade for Children and Youth: The New European Strategy for a Better Internet for Kids (BIK+)' (11 May 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0212>.

<sup>91</sup> Opening Statement from Niamh Hodnett, Online Safety Commissioner at Coimisiún na Meán [https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint\\_committee\\_on\\_children\\_equality\\_disability\\_integration\\_and\\_youth/sub\\_missions/2024/2024-02-20\\_opening-statement-niamh-hodnett-online-safety-commissioner-coimisiun-na-mean\\_en.pdf](https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_children_equality_disability_integration_and_youth/sub_missions/2024/2024-02-20_opening-statement-niamh-hodnett-online-safety-commissioner-coimisiun-na-mean_en.pdf).

<sup>92</sup> Including, although not limited to: Article 27 DSA "Recommender system transparency"; Article 28 "Online protection of minors"; Section 5 of the DSA (Articles 33–43) "Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks"

<sup>93</sup> 2009 Act, s.139K(2)(a).

<sup>94</sup> 2009 Act, s.139K(4)(a)–(b).

<sup>95</sup> 2009 Act, s.139M(c).

<sup>96</sup> 2009 Act, s.139M(f).

Codes should necessarily incorporate regulations on the use of recommender systems for children and young people, at a minimum.

### Recommendations

- **Require the Code to Regulate Recommender Systems of Child Users:** Ensure the Code explicitly includes regulations on recommender systems for child users (those under 18 years). This should include provisions to mitigate risks such as exposure to harmful content, excessive screen time, and the creation of harmful content ‘rabbit holes’.
- **Mandate Child-Specific Protections Related to Recommender Systems:** The Code should require providers implement a ‘disable-by-default’ setting for personalised recommendations for users under 18 years, with the ability to enable these features only when it is age-appropriate and/or subject to parental/guardian.
- **Prohibit Profiling of Children and young People:** Prohibit the use of recommender systems that rely on profiling of children and young people.
- **Use the Code to Support the Implementation of the DSA:** Ensure that the Code aligns with the Digital Services Act (DSA) and the Audiovisual Media Services (AVMS) Directive by including protections against the risks posed by recommender systems, particularly regarding content delivery and exposure to harmful material.
- **Enhance Transparency and Accountability:** Mandate that service providers implement transparent decision-making processes for recommender systems, clearly communicating how content is delivered to children and young people and how harmful content is moderated or prevented.
- **Ensure Swift Intervention for Harmful Recommender Content:** The Code should require providers to take immediate action when recommender systems expose children to harmful content, prioritising swift removal and mitigation measures to protect their well-being.

## 9. Illegal Content harmful to Children

Removing obligations relating to ‘Illegal Content harmful to Children’ from the Code fails to adequately reflect the obligations under Article 28b(1) DVMS Directive. According to the consultation document, the ‘illegal content covered by the revised draft Code has been narrowed.’<sup>97</sup> In fact, the illegal content covered by the Code has not simply been narrowed, but removed completely, with the exception of reference to three specific euro-crimes. Namely, public provocation to commit a terrorist offence,<sup>98</sup> offences concerning ‘child pornography’,<sup>99</sup> offences concerning racism and xenophobia,<sup>100</sup> and, separately, incitement to violence or hate on one of the protected grounds.<sup>101</sup> It is of particular note, that the offences relating to child sexual abuse that are included are ‘the distribution, dissemination or transmission of child pornography’.<sup>102</sup> This is considerably more narrow than the offences covered by Irish criminal law and does not reflect the breadth of serious sexual offences, such as where a person sends sexually explicit material to a child,<sup>103</sup> of sexual grooming of a child,<sup>104</sup> content by which a person communicates with another person for the purpose of facilitating the sexual exploitation of a child,<sup>105</sup> trafficking,<sup>106</sup> or threatening to share intimate images.<sup>107</sup>

What is now defined as ‘audiovisual commercial communications harmful to children’ in the revised Code is largely limited to audiovisual commercial communications: exhorting children to buy or hire a product or service by exploiting their inexperience or credulity; directly encourage children to persuade their parents or others to purchase the goods or services being advertised; exploiting the special trust children place in parents, teachers or other persons; unreasonably showing children in dangerous situations; for alcohol aimed specifically at children.<sup>108</sup>

According to the Coimisiún, the DSA ‘offers an appropriate avenue to address content that is illegal under the various specific Irish criminal offences’.<sup>109</sup> This is a narrow interpretation of obligations under the 2009 Act, and by extension the AVMS Directive. While these offence-specific online harms

<sup>97</sup> Response to Consultation: Online Safety Code

<sup>98</sup> As set out in Article 5 of Directive (EU) 2017/541, Revised Code, part 10.1(c)

<sup>99</sup> As set out in Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council, Revised Code, part 10.1(c)

<sup>100</sup> As set out in Article 1 of Framework Decision 2008/913/JHA Revised Code, part 10.1(c)

<sup>101</sup> Part 10.1(b) Draft Code

<sup>102</sup> Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council, Revised Code, part 10.1(c)

<sup>103</sup> section 8(2) of the Criminal Law (Sexual Offences) Act 2017

<sup>104</sup> Section 10, Criminal Law Sexual Offences Act 2017

<sup>105</sup> Contrary to s.8 (1) of the Criminal Law (Sexual Offences) Act 2017

<sup>106</sup> Section 3 Child Trafficking and Pornography Act 1998

<sup>107</sup> Schedule 3 2009 Act. While all the offences outlined in Schedule 3 may involve or impact on children there are specific offences that relate exclusively to children, these include: Online content by which a person communicates with another person for the purpose of facilitating the sexual exploitation of a child, contrary to section 8 (1) of the Criminal Law (Sexual Offences) Act 2017; Online content by which a person sends sexually explicit material to a child, contrary to section 8(2) of the Criminal Law (Sexual Offences) Act 2017; Online content by which a person exposes his or her genitals intending to cause fear, distress or alarm to another person contrary to section 45 (1) of the Criminal Law (Sexual Offences) Act 2017; 16. Online content by which a person publishes or includes in a broadcast a report to which section 51 (1) of the Children Act 2001 applies (report in relation to admission of a child to the Programme etc. or revealing information likely to lead to identification of the child); Online content by which a person publishes or includes in a broadcast any such report or picture as is referred to in section 93 (1) of the Children Act 2001, except so far as the requirements of that section have been dispensed with under subsection (2) of that section (proceedings before a court concerning a child: particulars likely to lead to identification etc.); Online content by which a person encourages unlawful activity involving a child, contrary to section 249 of the Children Act 2001 (person with custody, charge or care of a child encouraging sexual offences on the child etc.); Online content by which a person publishes or includes in a broadcast a report or picture to which section 252 (1) of the Children Act 2001 applies, except so far as the requirements of subsection (1) of that section have been dispensed with under subsection (2) of that section (proceedings for an offence against a child or where a child is a witness: report or picture likely to lead to identification of the child etc.); 14. Online content by which a person distributes, transmits, disseminates or publishes child pornography, contrary to section 5 (1)(b) of the Child Trafficking and Pornography Act 1998; Online content by which a person publishes, distributes, transmits or disseminates an advertisement, contrary to section 5 (1)(e) of the Child Trafficking and Pornography Act 1998 (advertisement of sale etc. of child pornography).

<sup>108</sup> S.11 Definitions, Revised Draft Online Safety Code

<sup>109</sup> Response to Consultation: Online Safety Code

may *also* be covered by obligations under the DSA this does *not* preclude Coimisiún from including these harms in the Online Safety Codes. In fact, s.139A (1) and (2) when read alongside Article 28B(1)(a) of the AVMS Directive requiring that measures to be taken to protect children and young people from harms that may impair their physical, mental or moral development would support the inclusion of naming the specific illegal content that is, at a minimum, harmful to children and young people in the Code. In contrast to the Code, s.139A of the 2009 Act (amended) defines ‘harmful online content’ as offence-specific categories of online content and non-offence-specific harmful online content.<sup>110</sup>

In the first draft of the Code, the Coimisiún clearly considered the child-specific approach to be of significant importance stating:

the AVMS Directive requires children to be protected from harm to their physical, mental or moral development. Coimisiún na Meán considers that the Code should be specific about the types of content that are considered to pose a risk of such harm. By providing a more specific definition, stakeholders have greater clarity about the scope of protection that the Code gives and VSPS providers have greater certainty about the scope of their legally binding obligations. The Code therefore contains definitions of ‘illegal content harmful to children’... The definition of ‘illegal content harmful to children’ comprises the relevant categories of offence-based harmful online content defined in the Act. This includes various types of content involved in sexual offences involving children, as well as illegal threats, harassment and grossly offensive communications where the victim is a child, or the content is likely to be seen by a child.<sup>111</sup>

As noted above, there is of course overlap between the DSA and the obligations under the AVMS Directive, the removal of offence-specific harmful content - specifically those relating to children and involving children - in the revised draft Code does not fully reflect the full ambit of ‘harmful online content’ as defined by the 2009 Act (the AVMS Directive) into the draft Code. Far from creating overlap between the DSA and the transposed AVMS Directive, including these offences in the Code has the potential to increase online safety for children and young people. It is worth repeating, that the DSA and the AVMS Directive are interlocking and mutually reinforcing pieces of legislation designed to enhance online safety, as a whole.

The DSA is of course broader in scope than the AVMS Directive,<sup>112</sup> covering content that is illegal under EU law and content that is illegal in national law. Where a breach is in contravention of national law, but not EU law, the European Commission has stated that content that is illegal only in a given Member State, as a general rule should only be removed in the territory where it is illegal.<sup>113</sup> Therefore, the argument that the large number of online platforms being headquartered in Ireland would result in the Irish Online Safety Code becoming the *de facto* EU-wide Code would not necessarily hold. If there is a commitment to protecting Irish users from harm online and in tackling the flow of illegal content then we must recognise the importance of including Irish criminal offences in the Online Safety Codes. This not only accords to Irish policy, but with a meaningful interpretation of the obligations under Article 28.(1)(a) of the AVMS Directive.

The Code, as currently drafted does not appear to be sufficiently child-centred. The narrowing of the definition of content harmful to children and the subsuming of other harmful content into a

---

<sup>110</sup> 138A (1)(a) and (b) 2009 Act

<sup>111</sup> Response to Consultation: Online Safety Code

<sup>112</sup> CERRE, *Overlaps between Data Protection and Competition Law* (CERRE, 2022) [https://cerre.eu/wp-content/uploads/2022/11/Overlaps\\_ReportFinal-2.pdf](https://cerre.eu/wp-content/uploads/2022/11/Overlaps_ReportFinal-2.pdf)

<sup>113</sup> European Commission, Questions and answers on the Digital Services Act, (February 2024) [https://dsa-observatory.eu/2023/11/01/the-extraterritorial-implications-of-the-digital-services-act/#\\_ftn1](https://dsa-observatory.eu/2023/11/01/the-extraterritorial-implications-of-the-digital-services-act/#_ftn1) Re copyright see UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (C-314/12). The court held that internet service provider (ISP) like UPC Telekabel can be considered intermediaries whose services are used to infringe copyright. Therefore, they can be required to block access to websites that make copyrighted works available to the public without the consent of the rights holders. Re jurisdiction see Google v Commission nationale de l’informatique et des libertés (CNIL) (Case C-507/17) in which the Court limited the jurisdiction to the EU, and Glawischnig-Piesczek v Facebook (Case C-18/18) wherein the Court did not limit the jurisdictional obligations to the EU.

‘restricted video content’, coupled with the removal of offence-specific harms relating to, or involving children will necessarily limit the obligations placed on AVMS platforms. Therefore, it follows that there are limited to no child-specific obligations placed on online platforms, save for the limited euro-crimes and commercial restrictions. As such, we are of the view that the Code cannot be said to ‘take appropriate measures to protect minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development’.<sup>114</sup>

### Recommendations

- **Include Offence-Specific Harms in the Code:** The Code should include offence-specific harms, particularly those involving children, such as sexual grooming, child sexual abuse, trafficking, and the sharing of intimate images. This will better align the Code with Irish law and with the obligations under Article 28b(1) of the AVMS Directive. This will ensure that online platforms are explicitly required to address illegal content specific to Irish law, reinforcing child safety.
- **Promote Consistency Between the DSA and AVMS Directive:** Ensure that the Code is consistent with both the Digital Services Act (DSA) and the AVMS Directive, recognising that these pieces of legislation are interlocking and mutually reinforcing in enhancing online safety, particularly for children.
- **Enhance Reporting Mechanisms for Child-Specific Harms:** The Code should require platforms to implement robust, transparent, and user-friendly reporting mechanisms specifically for child-related harms, including illegal content such as child sexual abuse material and online grooming. In addition, VSPS should be obligated to sign-post child and young users to specialist support services where they report such content.

---

<sup>114</sup> Article 28b(1)(a) AVMS Directive

## 10. Conclusion

---

While the revised Online Safety Code represents an important step toward safeguarding children and young people in Ireland's digital environments, further enhancements are necessary to fully align with the rights under the AVMS Directive and the UNCRC. The digital world presents both opportunities and significant risks for children and young people. Therefore, it is crucial that the Online Safety Code reflects a comprehensive and child-centred approach that prioritises their safety, well-being, and development.

The UNCRC sets forth specific rights that must be protected in both offline and online environments. Article 16 affirms the right to privacy, while Article 17 highlights the importance of access to appropriate information and protection from harmful material. Article 19 underscores the necessity of protecting children from all forms of physical and mental violence, abuse, and exploitation. Article 28 emphasises the right to education, including access to information and technology in a safe and supportive environment. The Online Safety Code must be aligned with these rights, ensuring that children's access to the digital world is not only safe but empowering, allowing them to benefit from the opportunities of the internet while being protected from its dangers.

To achieve this, the Code must include robust protections that reflect the unique vulnerabilities of children and young people. This includes ensuring that effective age assurance measures are in place, that responses to complaints and flags of content harmful to children or involving children is prioritised and responses are tailored to meet the needs of children, and children are protected from harmful content delivered through recommender systems. Moreover, it is important that the Code addresses offence-specific harms, especially those relating to child sexual exploitation, trafficking, and other illegal content harmful to children.

The Code must also recognise the evolving nature of digital technologies and the rapid pace at which new risks emerge. This necessitates a framework that is adaptable and able to respond to new challenges as they arise. Continuous evaluation and improvement of online safety mechanisms, including parental controls, privacy features, and content moderation systems, are key to keeping children and young people safe in a dynamic online environment. In addition, platforms must be held accountable for any failures in protecting children, with clear obligations to remove harmful content swiftly and to provide child-friendly complaint and reporting mechanisms that also offer information on specialist supports available.

By integrating these recommendations, the Online Safety Code can better serve as a powerful tool in protecting children and young people's rights online, ensuring that Ireland meets its obligations under national, EU and international law. This will not only contribute to making Ireland one of the best places in the world to be a child but will also set a strong example of leadership in digital child protection. Ultimately, this will help ensure that all children can safely engage with the digital world in a way that supports their development, well-being, and fulfilment of their rights as enshrined in the UNCRC.