

# Online Safety Monitor

Safeguarding Children's  
Rights Online



Education



Regulation



Rights

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  
Dpt. 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  
FASD Ireland  
Féach  
Focus Ireland  
Foetal Alcohol Spectrum Disorder (FASD) Ireland  
Foróige  
Gaeiloideachas  
Galway Traveller Movement  
GIY Ireland  
Good Shepherd Cork  
Helium Arts  
Humanist Association of Ireland  
Hygiene Hub  
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 Community Youth Service (KCYS)  
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  
Neurodiversity 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  
Sphere 17 Regional Youth Service  
SpunOut.ie  
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  
Treoir  
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

<b>ACKNOWLEDGEMENTS</b>	<b>4</b>
<b>GLOSSARY</b>	<b>5</b>
<b>INTRODUCTION/FOREWORD</b>	<b>6</b>
<b>SECTION 1: CHILDREN'S RIGHTS IN THE ONLINE WORLD</b>	<b>13</b>
<b>SECTION 2: ENFORCING REGULATION ON THE ONLINE INDUSTRY</b>	<b>23</b>
<b>SECTION 3: EDUCATION AND PREVENTION AGAINST HARM ONLINE</b>	<b>36</b>
<b>RECOMMENDATIONS</b>	<b>47</b>

## ACKNOWLEDGEMENTS

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 wishes to thank all those who contributed to researching and compiling this report. In particular, the Children's Rights Alliance would like to thank our partners Community Foundation Ireland and The Oak Foundation. The Children's Rights Alliance would like to thank our members and sector colleagues for their comments and co-operation in preparation of this report:

- CyberSafeKids
- The Irish Society for Prevention of Cruelty to Children (ISPCC)
- Sean Beatty BL, Catherine McGuinness Fellow with the Children's Rights Alliance and The Bar of Ireland (2024)

# GLOSSARY

## The Online Landscape

<b>AdTech</b>	Advertising Technology
<b>EdTech</b>	Educational Technology
<b>CSA</b>	Child Sexual Abuse
<b>CSAM</b>	Child Sexual Abuse Material
<b>VLOPs</b>	Very Large Online Platforms
<b>VLOSE</b>	Very Large Online Search Engine
<b>VSPS</b>	Video Sharing Platform Services

## The Regulatory Framework

<b>UNCRC</b>	United Nations Convention on the Rights of the Child, 1989
<b>OSMR Act</b>	The Online Safety and Media Regulation Act 2022
<b>An Garda Síochána</b>	Irish police force
<b>Coimisiún na Meán</b>	Regulator of broadcasting and online media in Ireland
<b>CRIA</b>	Child Rights Impact Assessments
<b>DSA</b>	The EU Digital Services Act 2022
<b>AVMSD</b>	The EU Audio-Visual Media Services Directive 2018
<b>CSA Directive</b>	EU Directive on combating the sexual abuse and sexual exploitation of children
<b>CSAM Regulation</b>	Proposed in 2022 by the EU Parliament and Council, the Regulation aims to lay down rules to prevent and combat child sexual abuse
<b>ODS</b>	Out-of-court dispute settlement bodies

# INTRODUCTION

The Online Safety Monitor 2025 is the first edition of a new annual series for the Children's Rights Alliance monitoring both online harms and the progress made by the State and the tech industry in better safeguarding children and young people's rights in digital environments. This foundational evaluation will provide an overview of children's rights online and how they have been implemented in laws and policies at both national and EU levels. This first edition focuses on the implementation of the Online Safety Codes in Ireland and the issue of online Child Sexual Abuse Material (CSAM) and exploitation in the context of proposed EU Regulation and Directives.

Since its beginning, the world wide web has rapidly developed both in terms of the technological advancements and in active global users. The online world is completely intertwined with the offline world and yet, until now, it has primarily been governed by its industry owners. The internet, online platforms and digital services have been created and controlled for maximum financial gain. They have not been built or designed with children's rights in mind and consequently, we have seen children and young people threatened, exposed, exploited, harmed, bullied and manipulated. In the most extreme cases, this has come at the ultimate cost of young lives.

Children's rights do not stop when they enter the online world or log on to a device. The evolving nature of technology must not outpace the rights and protections owed to children and young people. It is the responsibility of the State, the regulator, and industry to ensure that digital environments uphold, protect, and promote children's rights, rather than allow them to be compromised or undermined. It is unacceptable and legally and morally wrong to place all the emphasis onto children and their parents to protect them.

## Children's Rights Online

The unique rights of children and young people have been recognised as far back as the internet itself. In 1989, The United Nations Convention on the Rights of the Child was adopted setting out children's civil, political, economic, social, and cultural rights, ensuring their well-being, development, and participation in society.

As the digital world became increasingly central to children's lives, the need to extend the Convention to the digital space became all the more important. In 2021, the UN Committee on the Rights of the Child adopted General Comment No. 25. This General Comment focuses exclusively on children's rights in the digital environment, reinforcing their rights to information, education, participation, privacy, and protection from harm. By establishing a clear framework for assessing digital policies, the General Comment outlines the obligations owed by governments, businesses, and other stakeholders in creating online spaces that prioritise children's safety and inclusion while fostering their empowerment.

The UNCRC General Comment No. 25 establishes that the realisation of children's rights in the digital environment must be guided by four overarching principles, which underpin the implementation of all other rights under the Convention.<sup>1</sup>

---

1 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), paras 8-18.

1	That the best interests of the child must always be a primary consideration in all actions affecting children, including those in digital contexts <sup>2</sup>
2	The right to life, survival, and development underscores the need to ensure children's safety, well-being, and holistic development as they engage with digital platforms <sup>3</sup>
3	Non-discrimination requires that all children, regardless of their background or circumstances, have equal access to opportunities and protections in the digital environment, free from exclusion or bias <sup>4</sup>
4	Respect for the views of the child highlights the importance of recognising children as active participants in decisions affecting their lives, ensuring their voices are heard and valued, particularly in the development and implementation of digital policies <sup>5</sup>

In addition to the obligations under UNCRC, the Council of Europe *Guidelines to Respect, Protect, and Fulfil the Rights of the Child in the Digital Environment* require that 'in all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration'. The Guidelines further recommend that a fair balance be struck between the child's right to protection and their other rights to freedom of expression, participation, and access to information.<sup>6</sup> As part of this obligation, the States must establish regulations that reflect the particular vulnerabilities of children online, proactively ensuring that their best interests remain at the forefront of all legislative, policy, and service-related decisions.<sup>7</sup> This includes adopting preventive measures to protect children from online harms like exposure to violent content, data exploitation, and online grooming, as well as creating age-appropriate digital environments where children can learn, socialise, and express themselves safely.

The European Union legal framework is also relevant to child online safety, underpinned by fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (CFR).<sup>8</sup> Article 1 affirms human dignity,<sup>9</sup> which is crucial in protecting children from online harm, while Articles 6 to 8, 10 to 13 collectively safeguard fundamental freedoms, including; the right to liberty and security; respect for private and family life; protection of personal data; freedom of thought, conscience, and religion; freedom of expression and information; freedom of assembly and association; and freedom of the arts and sciences.<sup>10</sup> These rights are essential in ensuring child online safety, protecting privacy and digital rights, promoting access to information, and supporting children's participation and education in digital spaces, which would include digital literacy. Article 14(3) reinforces the right to education, which would include digital literacy, ensuring children can navigate online spaces safely.<sup>11</sup> Articles 20 and 21 guarantee equality and non-discrimination, including protection from risks such as cyberbullying and digital exclusion, ensuring all children have safe and equitable online experiences.<sup>12</sup>

2 *ibid*, para 12-13.

3 *ibid*, para 14-15.

4 *ibid* para 9-11.

5 *ibid*, para 16-18.

6 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)

7 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 12

8 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

9 *ibid* Article 1.

10 *ibid* Articles 6- 8, 10 -13.

11 *ibid* Article 14(3).

12 *ibid* Articles 20 and 21.

In addition, the European Convention on Human Rights (ECHR) which was incorporated into Irish law through the ECHR Act 2003, mandates under section 3 that all State Bodies, including regulators such as Coimisiún na Meán, uphold ECHR rights in their functions, thereby ensuring child online safety aligns with fundamental protections such as, for example, those under Article 8 (privacy) and Article 14 (non-discrimination).<sup>13</sup> Additionally, under section 42 of the Irish Human Rights and Equality Commission Act 2014 (IHREC Act 2014), the Irish Human Rights and Equality Commission (IHREC), as a public body, must proactively work to eliminate discrimination, promote equality, and protect human rights for all individuals in the State, including children navigating the digital environment.<sup>14</sup> Importantly, Article 42A.1 of the Irish Constitution recognises and affirms the natural and imprescriptible rights of all children, obligating the State to ensure their safety, which must also apply to digital spaces.<sup>15</sup>

The Monitor will apply the four principles set out in General Comment 25 to evaluate the actions Ireland has taken to protect and promote children's rights in the digital environment. This includes assessing whether these principles have been adequately integrated into Ireland's legislative and regulatory frameworks. The analysis will also identify gaps where additional measures are needed to align Ireland's approach with the requirements of UNCRC General Comment 25, ensuring that all children are equally protected and empowered in the digital age.

This Monitor examines critical areas impacting children's rights in the online world under three thematic areas:

- **Section 1: Children's Rights in the Online World**
- **Section 2: Enforcing Regulation on the Online Industry**
- **Section 3: Education and Prevention Against Harm Online**

**As digital engagement continues to grow, particularly among young people, the need for a robust framework to safeguard children's rights has never been greater.**

## The Online Landscape

As of February 2025, there are 5.56 billion people around the world using the internet.<sup>16</sup> In the last year alone, there were over half a million new active social media identities a day.<sup>17</sup> The social media dimension of the online landscape is alone, a multi-billion-dollar industry. The last few decades have reported rapid scale growth in terms of the number of people and the number of businesses now online. The problem is technological developments are outpacing the legislative and regulatory practices that set boundaries on this growth. Instead, big tech giants enjoyed years of self-regulation enabling them to set their own standards of operating, and importantly, their own parameters when it comes to addressing harms when they do occur on their sites. This legal leeway has failed to stop the rise of online hate, harassment and harm and it is young people who are most at risk of exposure.

<sup>13</sup> European Convention on Human Rights Act 2003, s 3.

<sup>14</sup> Irish Human Rights and Equality Commission Act 2014, s 42.

<sup>15</sup> Constitution of Ireland 1937, (Bunreacht na hÉireann) art 42A.1.

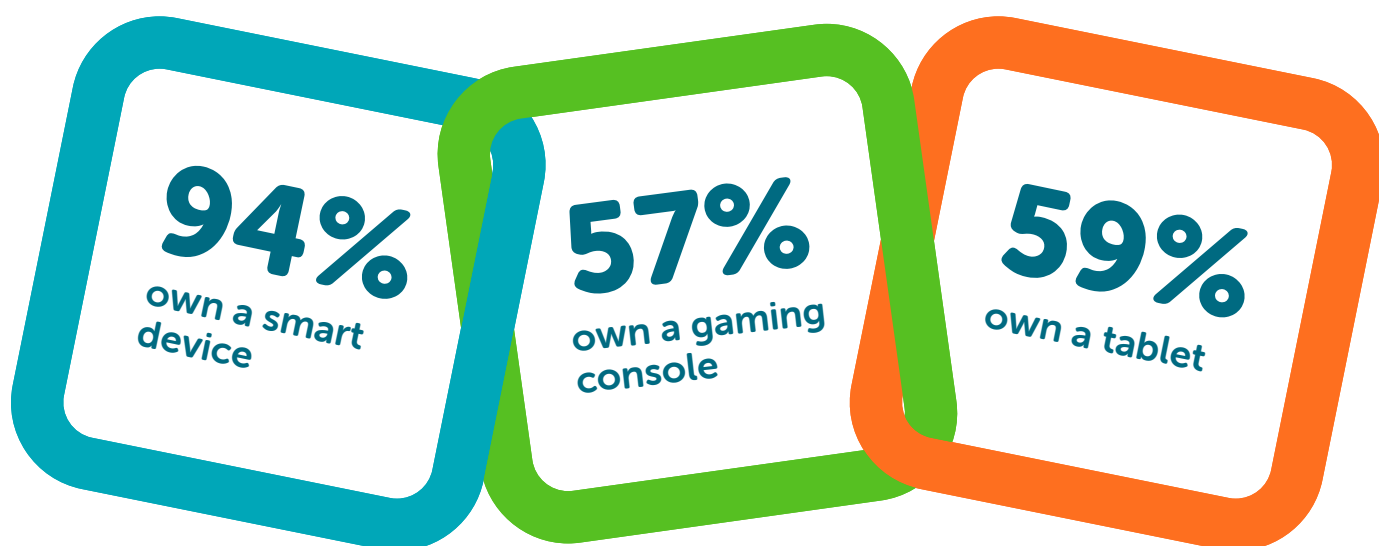
<sup>16</sup> Data RePortal, 'Digital Around the World' <<https://datareportal.com/global-digital-overview>> accessed 21 March 2025.

<sup>17</sup> *ibid*.



**Cyberbullying** is one of the most prevalent online harms children experience. Research by the National Anti-Bullying Research and Resource Centre found that 40 per cent of Irish children have experienced cyberbullying.<sup>18</sup> There is now increasing evidence of one of the most lucrative and profitable online industries', **pornography**, role in shaping and fuelling violence against women and girls.<sup>19</sup> In a recent Irish study, students reported first viewing pornography at a young age; 53.3 per cent of male students and 23.1 per cent of female students said they were aged 10 to 13 when they first viewed pornography.<sup>20</sup> Additionally, the former Special Rapporteur on Child Protection reported concerns about online grooming and exploitation facilitated by these platforms.<sup>21</sup> **Online child sexual abuse materials (CSAM)** and grooming, which involves manipulation to exploit and abuse individuals, are increasingly targeting younger children and spreading at an alarming rate. In 2023, reports of suspected online child sexual abuse reached a record 36.2 million, while grooming incidents surged by over 300 per cent between 2021 and 2023.<sup>22</sup> Most of the detected activities related to CSAM which was hosted in Europe<sup>23</sup> and almost all the content (99 per cent) was found on publicly available areas of the internet and was not hidden on the dark net.<sup>24</sup>

Ireland's young people are widely and deeply connected to the online world. Surveying children and young people themselves, (7,176 children, aged 8-14 years, in 101 schools across Ireland) CyberSafeKids' *Trends and Usage Reports*<sup>25</sup> give us an insight into what life online looks like for children and young people.



18 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.

19 Facing Reality: Addressing the role of Pornography in the pandemic of Violence against Women and Girls. Breslin R, O'Connor M. Sexual Exploitation Research and Policy Institute. October 2024 <<https://www.womensaid.ie/app/uploads/2024/10/Facing-Reality-Full-Report-October-2024.pdf>> accessed 31 January 2024.

20 Dawson, K., NicGabhainn, S., and MacNeela, P., 2021. Porn Report: Surveying Students on Pornography Use and Involving Them in Planning Critical Learning Interventions. Galway: NUI Galway

21 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 21 November 2024.

22 National Center for Missing & Exploited Children, '2023 CyberTipline Reports' (2024) <<https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf>> accessed 14 March 2025.

23 European Parliament, 'EU Legislation in Progress. A Brief', ((November 2024, available at <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS\\_BRI\(2022\)738224\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf)> accessed 04 March 2025

24 ibid.

25 CyberSafeKids, *Trends and Usage Report 2023-2024* (2024) <<https://www.cybersafekids.ie/wp-content/uploads/2024/08/CSK-TU-Report-23-24-Final.pdf>> accessed 13 December 2024, 11.

According to the National Survey of Children, their Parents and Adults regarding Online Safety, in 2021



of 12 year olds still in primary school education owned a smartphone



of 12 to 14 year olds in post primary school surveyed owned a smartphone



of Irish adolescents aged 15 to 17 owned a smartphone

Social media and messaging apps, with a minimum age rating of +13, continue to be prevalent amongst both:



**82%**  
of 8 to 12 year olds have their own accounts



**100%**  
of 12 to 14 year olds have their own accounts



of girls engage with **ROBLOX**



of boys play **FORTNITE**

Research conducted with 7,176 children, aged 8-14 years, in 101 schools across Ireland. CyberSafeKids, Trends and Usage Report 2023-2024 (2024).

The inherent risks of online platforms and digital services given the dominance of self-regulation for so many years, gives rise to concerns given the extent to which Irish children and young people are living their lives online. Worryingly, a third of children surveyed by CyberSafeKids (32 per cent of 7,176 children, aged 8-14 years, in 101 schools across Ireland) maintained private accounts only, representing a notable decrease from 39 per cent in the previous year.<sup>26</sup> Additionally, 19 per cent of those surveyed were unaware of their privacy settings, indicating a lack of familiarity with features that could offer increased protection.<sup>27</sup> There is also a growing inclination of children and young people to hide or withhold their negative interactions and experiences online. Research found that only 45 per cent of children surveyed reported upsetting online experiences to a parent or trusted adult; a decline from 54 per cent in previous years. Additionally, 36 per cent of children surveyed did not disclose these experiences to anyone, marking a 5 per cent increase from the previous year.<sup>28</sup> The absence of accessible complaints mechanisms or standard rules of content moderation and complaints handling has meant that children and young people have been left to fend for themselves, without a roadmap to on how to navigate the online landscape safely.

## The Regulatory Framework

We cannot escape the fact that the online landscape we are operating in is one populated with a vast number of children and young people. We also cannot ignore Ireland's unique position in this digital landscape. Ireland is home to the European headquarters for many of the major technology companies, including Apple, X (formerly Twitter), Google, Microsoft, Meta, Adobe, Amazon, Intel, and TikTok.<sup>29</sup> How Ireland respects the needs and rights of its children and young people, and responds to threats against their safety and wellbeing, matters on a much greater scale. Given the concentration of tech giants, the responsibility of Irish authorities to enforce national and international regulatory standards is paramount.<sup>30</sup> Effective oversight ensures compliance with children's rights frameworks, protecting user rights and shaping global best practices in digital governance.<sup>31</sup> Strong regulatory action in Ireland sets a global precedent, reinforcing the responsibility of technology companies to foster safer, more accountable digital environments.

It is not enough to acknowledge risks to children and young people; the State, industry leaders, educators, and civil society must act decisively to eliminate them. Research commissioned by the Children's Rights Alliance in 2021 found that 91 per cent of the public believe that the Government should stand up to the big tech companies and set rules that protect the public from harmful or illegal use. The Irish Government has taken strides towards making this happen, through the enactment of the Online Safety and Media Regulation Act 2022 and the establishment of Coimisiún na Meán, a new regulatory body tasked with overseeing online safety and media regulation. Ireland's Online Safety Commissioner was appointed in 2023 to ensure a dedicated focus on the online space in the new regulatory framework.

One of the first priorities for the new Commission was the development of the first legally binding Online Safety Code. Introduced in two parts, the Code will seek to establish baseline requirements for the most influential and powerful players in the online world to adhere to. Part A came into effect in November 2024 and imposes general obligations on the designated video-sharing platforms to safeguard all users, with additional obligations requiring platforms to provide protections for minors against content which may impair their physical, mental, or moral development. However, the Code largely leaves it to each of the regulated platforms to make their own decision as to what constitutes harmful or inappropriate content that may negatively impact children and young people.

---

26 CyberSafeKids, *Trends and Usage Report 2023-2024* (2024) <<https://www.cybersafekids.ie/wp-content/uploads/2024/08/CSK-TU-Report-23-24-Final.pdf>> accessed 13 December 2024, 8.

27 *ibid.*

28 *ibid.* Table 20.

29 Blathnaid O'Dea, 'Ireland is home to these 18 US tech titans – and they're hiring' (Silicon Republic, 4 July 2022) <<https://www.siliconrepublic.com/jobs-news/us-tech-companies-hiring-ireland>> accessed 11 March 2025.

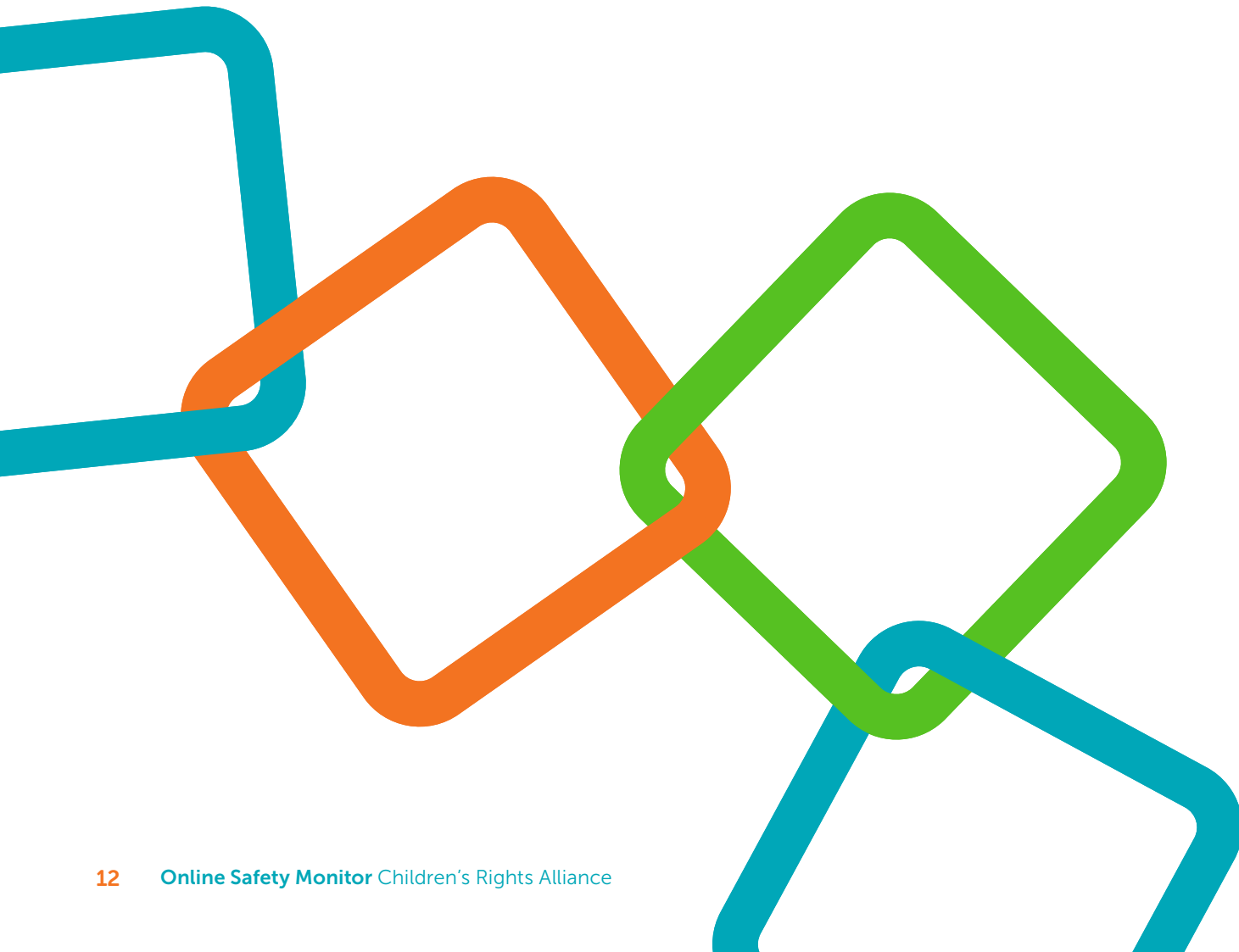
30 American Chamber of Commerce Ireland, *Regulating for Europe's Digital Future* (White Paper, 2024)

31 *ibid.*

Part B of the Online Safety Code comes into effect later this year and will include more stringent compliance measures for designated platforms on content considered to be restricted harmful content such as content encouraging bullying or humiliation, eating disorders, self-harm or suicide, or dangerous challenges, commercial communications targeting children and gratuitous violence and pornography. However, these terms remain undefined in the current Code.

At a European level, the Digital Services Act (DSA, 2022) marked a watershed moment in the decades-long campaign for more effective regulation of the online world. The DSA is fully applicable to all platforms from February 2024, with stricter measures in place for designated 'Very Large Online Platforms and Services' or those with more than 45 million users in Europe.

Progress has been made, but the reforms undertaken so far are not enough. Despite the introduction of these new laws and regulations, we are only on the cusp of a global movement to implement stronger and stricter measures to hold big tech and online companies accountable. To that extent, the frameworks are still partial, and child protection online remains inadequate. Without urgent and decisive action, children's digital rights will continue to be systematically undermined. By implementing the recommendations outlined in this report, Ireland can build a safer, more inclusive digital landscape that upholds children's rights and well-being in an increasingly digital world. The responsibility to create a safe, inclusive, and empowering digital world is not a matter of policy preference but a matter of human rights for children and young people.



## Section 1

# Children's rights in the online world



## SECTION 1: CHILDREN'S RIGHTS IN THE ONLINE WORLD

It has been well documented that children and young people face numerous harms online, including exposure to inappropriate content,<sup>32</sup> cyberbullying,<sup>33</sup> privacy violations,<sup>34</sup> and online grooming.<sup>35</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-to-12 use the internet, with 70 per cent accessing video-sharing platform services (VSPS) regularly.<sup>36</sup> Most social media platforms are considered a VSPS if they primarily enable users to upload, share, and view videos. While video-sharing platform services offer inclusion, educational, and entertainment opportunities, they also expose 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>37</sup> There is also increasing evidence of pornography's role in shaping and fuelling violence against women and girls.<sup>38</sup> Additionally, the former Special Rapporteur on Child Protection reported concerns about online grooming and exploitation facilitated by these

platforms.<sup>39</sup>

While the Online Safety and Media Regulation Act (OSMR Act) sets out the statutory framework for online safety, it does not impose a statutory obligation on service providers to prioritise the best interests of the child as a primary consideration in line with the principles outlined in General Comment No. 25 of the UN Committee on the Rights of the Child. This is a cornerstone principle for safeguarding children in digital environments,<sup>40</sup> and its omission constitutes a significant gap in Irish legislation. The OSMR Act includes provisions aimed at protecting children's rights, but the absence of an explicit legal mandate to prioritise the best interests of the child undermines the potential for robust and consistent protections. It is vital that all actions and decisions by service providers are fundamentally informed by a commitment to children's welfare and rights, with the best interests of the child being the primary consideration, making the inclusion of such a requirement essential for the protection and rights of children.

- 32 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-isshh/information societystatistics-households2020/>> accessed 22 July 2024.
- 33 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>> accessed 21 March 2025.
- 34 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 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.
- 35 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>> accessed 21 March 2025.
- 36 Central Statistics Office, 'Information Society Statistics – Households 2020' (CSO, 2020).
- 37 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.
- 38 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>> accessed 21 March 2025. 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>>accessed 21 November 2024.
- 39 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.
- 40 Children's Rights Alliance, 'Analysis of the Online Safety and Media Regulation (OSMR) Bill' (March 2022) <<https://childrensrights.ie/wp-content/uploads/2023/08/Analysis-of-the-Online-Safety-and-Media-Regulation-OSMR-Bill.pdf>> accessed 21 November 2024.

## Online Safety Codes

Ireland's Online Safety Code, published in October 2024, establishes binding rules for video-sharing platforms services (VSPS) headquartered in Ireland, such as Facebook, Instagram, TikTok and YouTube.

National regulators are bound by the obligation to ensure the best interest of the child when carrying out their regulatory duties.<sup>41</sup> A significant advance in this regard was the development<sup>42</sup> and publication of Ireland's first Online Safety Code in October 2024.<sup>43</sup> The Code sets binding rules applying to specified very large VSPS which have their EU headquarters in Ireland. Those designated for regulation under this Code by Coimisiún na Meán are; Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X (formerly Twitter), Pinterest, Tumblr, and Reddit.<sup>44</sup> The Code mandates these platforms to implement measures to protect users, especially children, from harmful content. This includes prohibiting the sharing of content related to cyberbullying, promotion of self-harm or suicide, eating disorders, incitement to hatred or violence, terrorism, child sexual abuse material, racism, and xenophobia. Platforms are also required to employ age verification systems to prevent minors from accessing adult content, provide parental controls for users under 16, and establish transparent reporting mechanisms for harmful content.<sup>45</sup>



- 41 United Nations 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 12-13.
- 42 Coimisiún na Meán seeks views for developing Ireland's First binding Online Safety Code July 2023. Coimisiún na Meán published consultation document: Online Safety December 2023. Coimisiún na Meán published revised (draft) Online Safety Code May 2024 along with a summary of the submissions received prepared by Wagner-Hatfield for the Commission.
- 43 Coimisiún na Meán, Online Safety Code (2024), <[https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean\\_Online-Safety-Code.pdf](https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf)> 21 November 2024.
- 44 Coimisiún na Meán, 'Coimisiún na Meán designates Video-Sharing Platform Services' (9 January 2024) <<https://www.cnam.ie/coimisiun-na-mean-designates-video-sharing-platform-services/>> accessed 4 November 2024.
- 45 Coimisiún na Meán, 'Coimisiún na Meán adopts final Online Safety Code' (21 October 2024) <<https://www.cnam.ie/coimisiun-na-mean-adopts-final-online-safety-code/>> accessed 11 March 2025.

The Online Safety Code transposes the EU Audiovisual Media Services Directive (AVMSD) (2018/1808/EU) into Irish law, aligning national regulations with EU-wide standards on video-sharing platforms. The AVMSD extends rules on harmful content, advertising, and platform accountability to digital services, ensuring consistent protections across Member States. Non-compliance with the Code can result in significant penalties, including fines of up to €20 million or 10 per cent of the platform's annual turnover, whichever is greater.<sup>46</sup>

In developing the Code, Coimisiún na Meán moved away from designating specific content as 'regulated content harmful to children' and 'illegal content harmful to children' in the Code despite both being in earlier iterations. Instead, these forms of harmful content are now subsumed within the definition of 'restricted content' and 'adult-only' content.<sup>47</sup> The State's obligation to protect children's rights both online and offline is grounded in the universal, indivisible, and inalienable nature of all human rights,<sup>48</sup> but nonetheless, children have special vulnerabilities and the lack of a child-specific focus in the Online Safety Code raises significant concerns about whether this commitment is being meaningfully upheld. The question is whether the expanded definition, which is not child-specific, is capable of effectively recognising and responding to the specific harms faced by children.

The international child rights organisation, the 5Rights Foundation, emphasises the critical role of age assurance in safeguarding and empowering children online. In their report, *But How Do They Know It's A Child?*, they recognise that age assurance is a crucial component of creating the digital world young people deserve;

driving the innovations and redesigns needed across the tech sector to support children's safe and meaningful participation online.<sup>49</sup>

As it stands, the Code contains a general obligation 'as appropriate, [to] establish and operate age verification systems with respect to content that may impair the physical, mental, or moral development of minors'.<sup>50</sup> However, such content remains undefined, and the obligation is extremely general and vague. How children and young people experience content will be different from how adults do. What is considered harmful to a child may not be so to an adult. While there is merit in the expansion to better protect all users online from such harmful content, it remains a concern that where such content involves children, or is encountered by them, the impact may be different, and if reported, the responses of the platforms may not now be sufficiently child specific.<sup>51</sup> As such, the Code's ability to protect children and young people online may be undermined where there is a general, not specific, requirement.

Coimisiún na Meán has also made a policy decision not to regulate platforms' application of algorithms and recommender systems through the Online Safety Code. Instead, the regulator will depend on the provisions of the Digital Safety Act (DSA).<sup>52</sup> Including recommender algorithms in the Online Safety Code would be a way of ensuring greater user protection by default, would align with strong public and international support, and would enhance the effectiveness of the Digital Services Act without compromising freedom of expression. Moreover, providers who have already complied with existing legal requirements should be able to ensure that recommender systems based on profiling are optional. As such, any

46 European Parliament and Council Directive (EU) 2018/1808 of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L 303/69.

47 Coimisiún na Meán, Online Safety Code (2024), <[https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean\\_Online-Safety-Code.pdf](https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf)> 21 November 2024, para 11.

48 Office of the High Commissioner for Human Rights, 'What Are Human Rights?' (OHCHR) <https://bangkok.ohchr.org/what-are-human-rights/> accessed 25 November 2024; Children's Commissioner for Scotland, 'What Does It Mean That Rights Are Interdependent?' <https://www.cypcs.org.uk/faq/what-does-it-mean-rights-interdependent/> accessed 25 November 2024.

49 5Rights Foundation, 'But How Do They Know It's a Child?' <<https://5rightsfoundation.com/resource/but-how-do-they-know-its-a-child/>> accessed 25 November 2024, 8.

50 Online Safety Code, para 10.6(f).

51 "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.

52 The Digital Services Act (DSA) establishes transparency requirements for recommender systems in Recital 70 and Articles 27, 34, 35, 38, 33-43 and 28.



implementation challenges would only arise for providers who have failed to meet these pre-existing legal obligations, making any difficulties a result of their own non-compliance rather than the measures of including such in the Code itself.<sup>53</sup> Research indicates that children often perceive online risks as inherent to their digital experiences, particularly on social media platforms, and exhibit a high tolerance for such exposure. Studies show that children are less likely to report content they identify as harmful or illegal.<sup>54</sup> As such, the complete absence of requirements for specific algorithmic safeguards, or requirements for privacy or VSPS product which is safe-by-design to protect child users from harmful behaviours or content from the Online Safety Code is concerning and will merit close and continuing attention to see whether the DSA is effective in guarding against these harms.<sup>55</sup>

The absence of a requirement that VSPS providers expedite and prioritise complaints relating to, involving, or made by children and young people is another significant gap. Instead, the primary responsibility continues to fall on children and young people using the service to understand the terms and conditions and, where these are breached, to lodge a complaint. It also falls on parents or caregivers to effectively manage the Parental Control mechanisms, which are only required for children under 16 years according to the Code.<sup>56</sup> This lack of prioritisation can leave children exposed to harm for longer, causing distress, anxiety, and possible escalation of the harm. Those with limited or

no parental support may be unable to get help, leaving them particularly vulnerable. Even with support from parents or caregivers, they may not have the knowledge or skill to recognise and report harmful content or may struggle to use the reporting systems effectively, leaving young people exposed to online risks.

The Online Safety Code requires platforms to prevent content on their platforms which breaches legislation common across the European Union, such as public provocation to commit a terrorist offence.<sup>57</sup> However, the offences relating to child sexual abuse that are included are 'the distribution, dissemination or transmission of child pornography' which is considerably narrower than the offences covered by Irish criminal law. Further, they do not reflect the breadth of serious sexual offences, such as; sending sexually explicit material to a child<sup>58</sup> sexual grooming of a child<sup>59</sup> content by which a person communicates with another person for the purpose of facilitating the sexual exploitation of a child<sup>60</sup> trafficking.<sup>61</sup> All of these criminal abuses of children remain outside the scope of the Code.

As a result, the Code lacks clear obligations for platforms to proactively manage illegal activity for the protection of children in digital spaces where they would be protected by Irish law if the offences happened offline. By narrowly defining illegal content, focusing predominantly on Euro-crimes such as the distribution of 'child pornography,' the Code inadequately addresses the full spectrum of child sexual exploitation offences under Irish law. While complementary

53 Irish Council for Civil Liberties and others, 'Joint Submission on the Draft Online Safety Code' (31 January 2024) <[https://www.iccl.ie/wp-content/uploads/2024/01/submission-60-civil-society-organisations-Coimisiun-na-Mean\\_OSC-Consultation-Response.pdf](https://www.iccl.ie/wp-content/uploads/2024/01/submission-60-civil-society-organisations-Coimisiun-na-Mean_OSC-Consultation-Response.pdf)> accessed 3 March 2025.

54 ECPAT International, *VOICE Report: Speaking Up for Change – Children's and Caregivers' Voices for Safer Online Experiences* (ECPAT International, 2024) <<https://ecpat.org/resource/voice-report-speaking-up-for-change-childrens-and-caregivers-voices-for-safer-online-experiences/> <<https://ecpat.org/resource/voice-report-speaking-up-for-change-childrens-and-caregivers-voices-for-safer-online-experiences/>> accessed 4 November 2024; Ofcom, *Children's Attitudes to Reporting Online Content* (Ofcom, 2024) <<https://www.ofcom.org.uk/online-safety/protecting-children/attitudes-to-reporting-content/>> accessed 4 November 2024.

55 Ding, K., Shen, Y., Liu, Q., and Li, H., *The Effects of Digital Addiction on Brain Function and Structure of Children and Adolescents: A Scoping Review*, National Library of Medicine, Dec 20, 2023 <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10779052/>> 9 Chang, M.L.Y., Lee, I.O., *Functional connectivity changes in the brain of adolescents with internet addiction: A systematic literature review of imaging studies*, PLOS, Jun 4, 2024 <<https://journals.plos.org/mentalhealth/article?id=10.1371/journal.pmen.0000022>>; Office of the U.S. Surgeon General, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, US Public Health Service, May 17, 2023, <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>. accessed 21 March 2025.

56 Online Safety Code May 2024, para 10.

57 As set out in Article 5 of Directive (EU) 2017/541, Revised Code, part 10.1(c).

58 Criminal Law (Sexual Offences) Act 2017, section 8(2).

59 Criminal Law Sexual Offences Act 2017, section 10. In a case that demonstrates the extreme harm a 26-year-old from Newry, was sentenced to life imprisonment for coercing thousands of young girls into sending explicit images, leading to the suicide of a 12-year-old victim. His case, one of the largest online sexual abuse investigations, see The Irish Times, 'Catfishing Case: Newry Man Whose Snapchat Threats Caused Death of Girl, 12, to Be Sentenced' (25 October 2024) <<https://www.irishtimes.com/crime-law/2024/10/25/catfishing-case-newry-man-whose-snapchat-threats-caused-death-of-girl-12-to-be-sentenced/>> accessed 10 March 2025.

60 Contrary to s.8 (1) of the Criminal Law (Sexual Offences) Act 2017.

61 Child Trafficking and Pornography Act 1998, section 3.

legislation<sup>62</sup> under the DSA requires hosting providers to report to national law enforcement or judicial authorities in cases involving threats to life or safety, the absence of naming such offences will make it less clear as to what this entails for both platform providers and users.

The *Online Safety Guidance Materials* document by Coimisiún na Meán provides guidelines to accompany the Online Safety Code. The document outlines non-binding recommendations designed to support video-sharing platform services in their implementation and adherence to the Code. The guidance relates to appropriate content moderation practices, age verification/assurance principles, recommended characteristics of parental controls, and user complaint handling. With a strong emphasis on child safety and public protection, the guidance also aligns with the EU's Digital Services Act, offering structured compliance expectations without enforcing proactive monitoring.<sup>63</sup> Although the *Online Safety Guidance Materials* set out useful recommendations, they ultimately leave much of the decision-making on child protection and safety to the platforms themselves, leading to a high likelihood of inconsistent implementation and potentially uneven protection standards across services. Despite these guidelines, gaps in protections for children and young people remain as VSPS providers are permitted to continue to set their own standards on issues like age verification without clear baselines or targets from Coimisiún na Meán.<sup>64</sup>

Not all of the obligations of the Code came into effect in November 2024. Part A of the Code took effect in November 2024, but designated platforms have until July 2025 to deliver their proposed solutions on such matters as age-verification under Part B; delaying the full regulatory protection of the Code.<sup>65</sup> This delay prolongs the risks faced by children and young

people, leaving them exposed to potential online harms without the full safeguards intended by the regulation. In the meantime, inconsistent protections across platforms may create further confusion and vulnerabilities for young users.

## Right to Life, Survival, and Development

All children have the right to be safe and protected from harm. Under the UNCRC, States must ensure children's right to life, survival, and development.<sup>66</sup> Article 19 requires States to adopt measures to shield children from physical or mental violence, abuse, neglect, and exploitation. States are also required to prevent all forms of sexual exploitation and abuse, including coercion into unlawful sexual activities, exploitative prostitution, and pornographic involvement.<sup>67</sup> General Comment No. 25 on the Convention reinforces those statements of rights by clarifying that the State must take measures to prevent online exploitation and ensure platforms have mechanisms for reporting and addressing abuse, and protecting children from harm in digital and physical spaces.<sup>68</sup>

The UNCRC emphasises the need to respect the evolving capacities of young people; adapting protections and opportunities in the digital environment according to age and development.<sup>69</sup> Article 16 safeguards children's privacy, while Article 17 protects their access to beneficial information and protection from harmful content; encouraging media literacy to help children make informed online choices.<sup>70</sup> Article 28 asserts the right to education, including safe digital access so children can benefit from online opportunities while being shielded from risks.

62 Digital Services Act (DSA), Article 18.

63 Coimisiún na Meán, *Online Safety Guidance Materials* (October 2024) <<https://www.cnam.ie/wp-content/uploads/2024/10/Online-Safety-Guidance-Materials.pdf>> accessed 6 November 2024.

64 Children's Rights Alliance, *Response to the Revised Online Safety Code* (Children's Rights Alliance, August 2024) <<https://childrensrights.ie/wp-content/uploads/2024/09/Childrens-Rights-Alliance-Response-to-the-Revised-Online-Safety-Code.pdf>> accessed 31 October 2024.

65 Coimisiún na Meán, *Online Safety Code Questions and Answers* (21 October 2024) <[https://www.cnam.ie/wp-content/uploads/2024/10/20241021\\_OSC\\_QA-1.pdf](https://www.cnam.ie/wp-content/uploads/2024/10/20241021_OSC_QA-1.pdf)> accessed 6 November 2024.

66 UNCRC, art 6.

67 UNCRC, art 34.

68 UNCRC art 19; United Nations 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 paras 25, 35.

69 United Nations 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 paras 19-21.

70 United Nations 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 50.

While it can be acknowledged that progress has been made in advancing obligations such as the right to protection from harm through the passing of the OSMR Act which imposes various duties to safeguard children,<sup>71</sup> and through EU law,<sup>72</sup> there remain significant gaps in meeting the obligations owed to children. Particularly in securing their right to privacy, accurate information, digital literacy, recognising their evolving capacity and education.<sup>73</sup> It is clear that not all children's rights are advancing, and some are falling behind. Strong protections are still lacking, and much more needs to be done to safeguard their rights effectively.

## Respect for the Views of the Child

All children have the right to have their views heard in all matters affecting them, including the digital environment.<sup>74</sup> General Comment No. 25 of that Convention requires that children be afforded the crucial opportunities for their voices to be heard in matters that affect them.<sup>75</sup> The use of digital technologies can help to realise children's participation at the local, national, and international levels.<sup>76</sup> States are required to promote awareness of, and access to, digital means for children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed, so that they can be effective advocates for their rights, individually and as a group.<sup>77</sup>

In line with the requirements of the OSMR Act,<sup>78</sup> Coimisiún na Meán established the Youth Advisory Committee from the outset in 2023 to incorporate the perspectives of young people into policies aimed at online safety. It is worth noting this is the only place within the OSMR Act that requires consultation or direct participation by children and young people.<sup>79</sup> The Youth Advisory Committee comprises representatives from nine national youth organisations and nine individuals under 25 years of age.<sup>80</sup> The Committee has convened on several occasions since its inaugural meeting on 19 December 2023. These meetings included a focus on the draft Online Safety Code and related guidance materials, addressing issues such as protections against harmful online content, including cyberbullying and materials promoting self-harm.<sup>81</sup> It is also welcome that Coimisiún na Meán intends to extend the Committee's membership to include participants who are under 18 years, ensuring a broader representation of youth perspectives in shaping online safety regulations. In addition, many organisations working with and for children contributed to the public consultations on the development of the Online Safety Code and other digitally focused consultations.

- 
- 71 The Online Safety and Media Regulation Act 2022 includes several provisions aimed at protecting children from harmful online content. The key sections addressing child protection are: section 7(2)(b), section 7(4)(a) and section (4)(d)(iii). In relation to the making of codes for on-demand services section 46N and section 46(2)(c)(i). In the designation of online services to which the online code is application section 139E(3)(f), section 139K(2)(d) and section 139M(f).
- 72 The DSA supports these obligations by requiring in Article 28(1) that platforms accessible to children to 'put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors' and in EU's Article 28(b) AVMS Directive Audio-Visual Media Services Directive mandating protections from harmful media content. Together, these regulations aim to balance children's safety with their right to access and benefit from the digital world.
- 73 The Online Safety and Media Regulation Act 2022 includes several provisions aimed at protecting children from harmful online content. The key sections addressing child protection are: section 7(2)(b), section 7(4)(a) and section (4)(d)(iii). In relation to the making of codes for on-demand services section 46N and section 46(2)(c)(i). In the designation of online services to which the online code is application section 139E(3)(f), section 139K(2)(d) and section 139M(f).
- 74 UNCRC, art 12.
- 75 5Rights Foundation, *Our Rights in a Digital World: Full Report* (September 2024) <<https://5rightsfoundation.com/wp-content/uploads/2024/09/OurRightsinaDigitalWorld-FullReport.pdf>> accessed 6 November 2024, 17.
- 76 UNCRC, General Comment 14 (2013), paras. 89–91.
- 77 UNCRC General Comment No. 25, para 16.
- 78 Section 19(9) Broadcast Act 2009 (as amended by the OSMR Act).
- 79 With one exception which relates to the public broadcaster which sets out the possibility of conducting a survey of children and young persons, for the purpose of ascertaining the views and interests of children and young persons in respect of public service broadcasting by the corporation', see section 96(11) Broadcasting Act 2009 (amended).
- 80 BeLong To; Children's Rights Alliance; CyberSafeKids; Irish Traveller Movement; ISPPCC National Parents Council; National Youth Council of Ireland; spunout; Webwise, see Coimisiún na Meán, 'Coimisiún na Meán Holds First Meeting of Youth Advisory Committee' (19 December 2023) <<https://www.cnam.ie/coimisiun-na-mean-holds-first-meeting-of-youth-advisory-committee/>> accessed 4 November 2024.
- 81 Coimisiún na Meán, 'Report of the Youth Advisory Committee (May 2024)' (May 2024) <<https://www.cnam.ie/wp-content/uploads/2024/05/Youth-Advisory-Committee-Report.pdf>> accessed 4 November 2024.

## Non-Discrimination

Children have the right to enjoy all rights without discrimination based on race, sex, disability, or any other status.<sup>82</sup> This extends to the digital sphere, where the State must address digital exclusion and ensure equitable access to digital resources, particularly for children from marginalised communities. General Comment No. 25 of the UNCRC stresses that children should not face discriminatory practices, including biased algorithms or exclusionary access, in their engagement with digital technologies.<sup>83</sup> The State has a responsibility to ensure that children from all backgrounds, particularly those from vulnerable groups, are protected from discrimination and exclusion in the digital environment.

The report published by the *Council of Europe, Two Clicks Forward and One Click Back: Report on Children with Disabilities in the Digital Environment*, provides important guidance on inclusivity and safety in digital spaces for children with disabilities.<sup>84</sup> It recommends that laws and policies be regularly reviewed to address the specific needs of children with disabilities effectively.<sup>85</sup> Schools should be provided with guidance, advice, and resources to utilise a wide range of available assistive and technological tools. As protective measures are developed against online abuse, harassment, cyberbullying, grooming, and other potential online harms, it is essential that the unique risks faced by children with disabilities, especially those with intellectual impairments, are expressly included.<sup>86</sup> Government-provided information on online safety must be accessible in formats that cater to these children, including easy-to-read versions and accessible reporting methods.<sup>87</sup> Additionally, tailored online safety and protection

information should be available to parents, guardians, educators, and professionals working with children with various types of special needs.<sup>88</sup> The State must actively involve children with disabilities in designing and implementing policies and services that impact their digital access and experiences.<sup>89</sup> The report also found that legislation may be necessary to require or encourage both public and private entities to review their policies, services, products, and resource allocation to ensure non-discriminatory access to the digital environment for children with disabilities.<sup>90</sup>

Ireland has implemented the EU Web Accessibility Directive<sup>91</sup> requiring public sector bodies to ensure that their websites and apps are accessible to users, especially people with disabilities, by making them perceivable, operable, understandable, and robust. The regulations came into force on 23 September 2020 as a necessary step to ensure that users, including children, can access the information and knowledge that they need. The National Disability Authority is the national monitoring body under these regulations.<sup>92</sup> As Coimisiún na Meán is a new agency, no public assessment of its accessibility has yet been issued.

*Ireland's Literacy, Numeracy and Digital Literacy Strategy 2024-2033*,<sup>93</sup> published in May 2024, commits to inclusive education to improve, amongst other indicators, digital literacy for all learners.<sup>94</sup> It specifically notes that children for whom English is a second language, or children from different ethnic and cultural backgrounds, including Traveller and Roma children, may be at risk of educational disadvantage. The risk of discrimination and exclusion of Traveller and Roma children is further noted in the *Traveller and Roma Education Strategy* published in July

82 UNCRC, art 2.

83 *ibid.*

84 Laura Lundy, Bronagh Byrne, Michelle Templeton, and Gerison Lansdown, *Two Clicks Forward and One Click Back: Report on Children with Disabilities in the Digital Environment* (Council of Europe 2019) <<https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f>> accessed 30 October 2024.

85 *ibid.*, 18.

86 *ibid.*

87 *ibid.*

88 *ibid.*

89 *ibid.*

90 *ibid.*

91 S.I. No. 358/2020 - European Union (Accessibility of Websites and Mobile Applications of Public Sector Bodies) Regulations 2020.

92 National Disability Authority, 'EU Web Accessibility Directive' <<https://nda.ie/monitoring/eu-web-accessibility-directive>> accessed 21 March 2025.

93 Department of Education, 'Ministers Foley and O'Gorman launch Ireland's Literacy, Numeracy and Digital Literacy Strategy 2024-2033' (gov.ie, 15 May 2024) <<https://www.gov.ie/en/press-release/40842-ministers-foley-and-minister-ogorman-launch-irelands-literacy-numeracy-and-digital-literacy-strategy-2024-2033/>> accessed 6 November 2024.

94 *ibid.*

2024, which highlighted the need for additional resources for Traveller and Roma children and their parents, guardians, and community. Both strategies are in the early stages of implementation.<sup>95</sup> These strategies should help to advance the rights of children at risk of exclusion. If effectively implemented, these strategies have the potential to ensure equal access to education, improving digital literacy, and reducing barriers faced by marginalised children. By providing targeted resources and support, they can promote inclusion, prevent discrimination, and empower children with the skills needed to participate fully in society.

Importantly, the Irish Traveller Movement (ITM) successfully advocated for Travellers to be explicitly protected in the Online Safety Code and are a member of the Coimisiún na Meán Youth Advisory Committee. However, they remain concerned that gaps remain, particularly in addressing harmful content that perpetuates stereotypes and systemic racism without explicit incitement. Algorithm-driven harm continues to expose Traveller children to identity-based discrimination and hate, with recommender systems amplifying harmful content. ITM urges stronger platform regulations, proactive safeguards beyond complaints-based processes, and broader definitions of hate to ensure real-time protection across all platforms.<sup>96</sup>



95 *ibid.*

96 Information received by the Children's Rights Alliance from the Irish Traveller Movement, 10 February 2025.



## Children's Rights in the Online World: Recommendations

- Amend Online Safety and Media Regulation (OSMR) Act to require the best interests of the child be the primary consideration in all aspects of online regulation and implementation, ensuring domestic alignment with these international obligations.
- Coimisiún na Meán's Youth Advisory Committee should be expanded without delay to include under-18s, ensuring direct child representation in online safety policy development.
- Online safety initiatives must include marginalised children, including Traveller and Roma children, children with disabilities, LGBTQI+ youth, and those from low-income backgrounds. Accessible, inclusive resources should be sustained and expanded, with tailored support for parents, caregivers, and educators to protect children online.

## Section 2

# Enforcing regulation on the online industry



## SECTION 2 – ENFORCING REGULATION ON THE ONLINE INDUSTRY

Opportunities for the realisation of children’s rights and their protection in the digital environment require a broad range of legislative, administrative and other measures, including precautionary ones.<sup>97</sup> The UN Convention on the Rights of the Child (UNCRC) General Comment requires that States ‘...take all appropriate measures to protect children from risks to their right to life, survival and development. Risks relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist.’<sup>98</sup>

In addition, children’s online protection should be integrated within national child protection policies.<sup>99</sup> States should implement measures that protect children from risks such as cyberaggression and digital technology-facilitated and online child sexual exploitation and abuse, and ensure the investigation of such crimes, and provide remedies and support for children who are victims.

The guidance from UNCRC General Comment No. 25 also recommends co-ordination across Government. Such a national coordination mechanism should engage with schools and the information and communications technology sector, and cooperate with businesses, civil society, academia, and organisations to realise children’s rights in relation to the digital environment at the cross-sectoral, national, regional, and local levels. It also requires States to ensure that there are sufficient public resources allocated to implement legislation, policies, and programmes to fully realise children’s rights in the digital environment.<sup>100</sup>

Further, UNCRC General Comment No. 25 notes that children face particular challenges in accessing justice in the digital environment. States are required to put appropriate and effective mechanisms in place and make them readily available for violations of children’s rights in the online environment.<sup>101</sup>

### National and EU Regulation

In recent years, the protection of children and young people’s rights online have been considered by legislators and policy makers in Ireland and in the European Union. The development of legislation has tended to develop along similar paths at EU and at Member State level with a view to ensuring smooth regulation across the Union and equality of protection for services accessed throughout the territory of the Union.

#### *Online Safety and Media Regulation Act*

As a result, a series of robust legal and regulatory advancements have created a complex framework for online safety in Ireland. Led by the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, the enactment of the Online Safety and Media Regulation Act 2022 (OSMR Act) established a framework for regulation of online safety for every Irish user, with a special focus on children. The Act also incorporated the EU Audiovisual Media Services Directive (AVMSD).<sup>102</sup>

That Act established Coimisiún na Meán as the regulatory authority for media and online safety.<sup>103</sup> A key role within this body is that of the Online Safety Commissioner, responsible for creating and implementing binding Online Safety Codes that apply to large digital platforms hosting audio-visual media services content and indissociable content.<sup>104</sup> These codes address

97 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children’s rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 22.

98 *ibid*, para 14.

99 Department of Children, Equality, Disability, Integration and Youth, *Children First: National Guidelines for the Protection and Welfare of Children* (2017).

100 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children’s rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), paras 22-28.

101 *ibid*, paras 43-44.

102 Directive (EU) 2018/1808 (Amendment to the AVMSD) <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN>> accessed 3 March 2025.

103 Online Safety and Media Regulation Act 2022.

104 Coimisiún na Meán, Online Safety Code (October 2024).



harmful content, including cyberbullying and content promoting self-harm,<sup>105</sup> with stringent penalties for non-compliance, such as fines or service blocks.<sup>106</sup> The OSMR Act also transposed the AVMSD, expanding statutory regulation to include video-sharing and on-demand media services. The OSMR Act obliges designated platforms to adhere to rules on advertising, age-appropriate content, and accessibility.<sup>107</sup>

Additionally, through another EU Regulation, the Digital Services Act (DSA) designated Coimisiún na Meán as Ireland's Digital Services Coordinator in February 2024.<sup>108</sup> This important role requires them to enforce EU standards on transparency, illegal content, and disinformation. This framework has the potential to enhance protections for children by reducing their exposure to harmful and inappropriate content, strengthening age-verification measures, and increasing platform accountability in fostering a safer online environment.

### Online Safety Code

Following its establishment in March 2023, Coimisiún na Meán published Ireland's first Online Safety Code on 21 October 2024, which is being phased in in two stages. The first, Part A, effective 19 November 2024, imposes general obligations on video-sharing platforms<sup>109</sup> to safeguard all users, with additional obligations requiring platforms to provide protections for minors against content which may impair their physical, mental, or moral development.<sup>110</sup> While it largely leaves it to the regulated platforms to decide what constitutes content which could

impair children's development, the Code states that 'for the purposes of the protection of minors, provided for in Article 28b(1)(a) of the Directive, the most harmful content shall be subject to 'the strictest measures''.<sup>111</sup>

Part B of the Code, introducing more detailed compliance measures, is due to come into force by 21 July 2025. Between October 2024 and July 2025, the regulated platforms<sup>112</sup> are to furnish Coimisiún na Meán with a scheme of measures suitable for each platform individually, to address the overall objective of restricting and removing illegal and harmful content. This part of the regulations specifies 'restricted harmful content' as content that encourages eating disorders, content that promotes or encourages self-harm or suicide, or dangerous challenges where such that the content meets the 'risk test' as defined in the Code.<sup>113</sup> This part of the Code also specifies that gratuitous violence and pornography are to be subject to the strictest restrictive measures. However, these terms remain undefined and therefore at the discretion of the platforms pending Coimisiún na Meán forming a view and either agreeing or challenging platforms on it.

Given that in the Code certain content is specifically designated as 'adult-only' and the specific measures required to protect children, it necessarily requires some form of age-verification, yet this is undefined. While Part A contains a general obligation on video-sharing platform services (VSPS) to 'establish and operate age verification systems for users of VSPS with respect to content which may impair the physical, mental or moral development of

105 Section 139A Broadcasting Act 2009 (as amended by the 'Online Safety and Media Regulation Act 2022).

106 *ibid*, Section 139K.

107 Section 139ZS of the Broadcasting Act 2009 (as amended by the 'Online Safety and Media Regulation Act 2022) empowers Coimisiún na Meán to impose financial sanctions on designated online services that fail to adhere to these Codes. These penalties can be as high as €20 million or 10 per cent of the provider's turnover from the previous financial year, depending on which amount is greater. Section 139ZW Broadcasting Act 2009 (as amended by the 'Online Safety and Media Regulation Act 2022. The Act allows for additional enforcement actions, such as ordering the removal of harmful content or even blocking access to non-compliant services if necessary under section 139ZC Broadcasting Act 2009 (as amended by the 'Online Safety and Media Regulation Act 2022).

108 Department of Enterprise, Trade and Employment, 'Minister Coveney Announces the Commencement of the Digital Services Act 2024' (gov.ie, 19 February 2024) <<https://www.gov.ie/en/press-release/71c6a-minister-coveney-announces-the-commencement-of-the-digital-services-act-2024/>> accessed 31 October 2024.

109 The Online Safety Code applies to video-sharing platforms headquartered in Ireland, including Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X (formerly Twitter), Pinterest, Tumblr, and Reddit. Coimisiún na Meán, 'Coimisiún na Meán Designates Video-Sharing Platform Services' (Coimisiún na Meán, 11 March 2024) <<https://www.cnam.ie/coimisiun-na-mean-designates-video-sharing-platform-services/>> accessed 03 March 2025.

110 Coimisiún na Meán, Online Safety Code (October 2024), section 10 transposing Article 28b(1)(a)-(c) AVMS Directive.

111 *ibid*, section 10.8.

112 The Online Safety Code applies to video-sharing platforms headquartered in Ireland, including Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X (formerly Twitter), Pinterest, Tumblr, and Reddit. Coimisiún na Meán, 'Coimisiún na Meán Designates Video-Sharing Platform Services' (Coimisiún na Meán, 11 March 2024) <<https://www.cnam.ie/coimisiun-na-mean-designates-video-sharing-platform-services/>> accessed 03 March 2025.

113 Coimisiún na Meán, Online Safety Code (October 2024) Part B.

minors',<sup>114</sup> it is only Part B of the Code which explicitly requires the platforms to produce proposals as to how they will verify the age of users. That more detailed requirement of age-verification relates solely to 'adult-only content', being video material featuring pornography or realistic depictions of extreme violence or cruelty. However, as noted above, none of those terms are defined, either in the Code or in the *Statutory Guidance*.<sup>115</sup>

This narrow and vague definition limits the requirement for age verification to platforms that explicitly permit adult-only content, leaving many of the mainstream platforms where children risk viewing harmful and illegal content subject only to the general obligations in Part A, as outlined above. This then raises concerns about the adequacy of age safeguards across platforms.<sup>116</sup> *The Online Safety Guidance Materials*<sup>117</sup> outline age assurance requirements but lack specific standards, leaving platforms considerable discretion to choose methods such as credit cards, AI-driven facial analysis, and behavioural profiling, without clear reliability or privacy safeguards.<sup>118</sup> Although the guidance prohibits self-declaration<sup>119</sup> and recommends privacy protections for children's data, it fails to specify how platforms should secure this data when using AI-based or data-intensive techniques.<sup>120</sup>

The approach taken by the Coimisiún na Meán aims to require the platforms to engage seriously with the regulator in producing a scheme of measures, suitable for each platform individually to address the overall objective of restricting and removing illegal and harmful content.

Overall, in addition to the concern that many of these measures may not be adopted by the companies until July 2025, there is insufficient direction in the Code as it stands requiring the platforms to adopt child rights sufficient standards to ensure that material which might

impair or damage the physical, mental, or moral development of children is effectively restricted. Even where the Code states that 'for the purposes of the protection of minors' the most harmful content shall be subject to 'the strictest measures', those measures are not defined.

While Coimisiún na Meán is still in its start-up phase and building its capacity, it must ensure it has sufficient resources to effectively engage with and monitor regulated platforms. This is essential to uphold children's rights regarding age verification, child-centred product and system design, and the provision of speedy, safe, and accessible complaint mechanisms.

### *Criminal Offences*

While Part A of the Online Safety Code requires platforms to protect users, including children, from disseminating material that constitutes an activity which is a criminal offence under European Union law,<sup>121</sup> no such protection exists for certain Irish offences which can result in child harm. This is despite the fact that the Irish OSMR Act 2022 specifies a list of offence-specific categories of harmful online content.<sup>122</sup> Among the many Irish crimes covered are: 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; and 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. These are but two of the many listed in the Irish legislation that illustrate the concern of the Oireachtas to ensure that protection was widespread.

The rationale for not including these specifically in the Online Safety Code is that dissemination of illegal material, including material relevant to

114 *ibid*, section 10.6(f).

115 Coimisiún na Meán, *Online Safety Guidance Materials* (October 2024).

116 Section 10.6(f) of the online Safety Code reads '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 minor'.

117 Coimisiún na Meán, *Online Safety Guidance Materials* (October 2024).

118 *ibid*, 13.

119 *ibid*, 12.

120 The standards developed by the 5Rights Foundation set out 11 common standards that should inform the development of any age assurance mechanism. Those are: Age assurance must be privacy preserving; Age assurance should be proportionate to risk and purpose; Age assurance should be easy for children to use; Age assurance must enhance children's experiences, not merely restrict them; Age assurance providers must offer a high level of security; Age assurance providers must offer routes to challenge and redress; Age assurance must be accessible and inclusive; Age assurance must be transparent and accountable; Age assurance should anticipate that children don't always tell the truth; Age assurance must adhere to agreed standards, 5Rights Foundation, *But How Do They Know It is a Child? Age Assurance in the Digital World* (5Rights Foundation, 2021) 8.

121 Coimisiún na Meán, *Online Safety Code* (October 2024), section 10.1(c).

122 Online Safety and Media Regulation Act 2022, s46.

these offences is covered by another aspect of the Irish regulatory regime, the Digital Services Act (DSA). However, the DSA does not define what constitutes illegal content and instead relies on existing EU or national laws, such as terrorist content, child sexual abuse material, and illegal hate speech, which are defined at the EU level. Although if content is illegal only in a specific Member State, it is generally removed only within that country. The lack of clarity creates challenges for platforms trying to comply with national laws. Excluding the list of scheduled offences from the Online Safety Code is a missed opportunity to clarify which offences apply. A defined list would provide legal certainty and ensure more consistent enforcement.<sup>123</sup>

However, so far, the standards required by the DSA are also subject to interpretation by regulation and by platforms. To shape effective guidelines for use by the platforms, the European Commission has initiated a consultation process specifically on Article 28 of the DSA,<sup>124</sup> collecting feedback from stakeholders, including children's rights groups, digital rights advocates, and industry representatives and is aiming for further public consultation in early 2025 and guideline finalisation by mid-2025. Input from organisations such as Eurochild and the 5Rights Foundation emphasised the need for the guidelines to include mandatory child rights assessments, restrictive data practices, and protections against harmful design features to safeguard young users' online experiences.<sup>125</sup>

### *Child Sexual Abuse Material*

Alongside these regulatory reforms, the EU has been intensifying its efforts to combat child sexual abuse material (CSAM) through a new proposed Regulation and updates to existing frameworks, including the recasting of the 2011 Child Sexual Abuse Directive (formerly known as the Child Pornography Directive).

There is widespread agreement that child sexual abuse (CSA) is a particularly serious crime and a major public health problem that has wide-ranging and serious life-long consequences for victims.<sup>126</sup> In hurting children, these crimes are a breach of children's rights, and cause significant and long-term social harm to them, their communities, and their societies. Advancements in digital technology make it increasingly difficult to prevent and detect crimes, as perpetrators continually find new ways to exploit these innovations.<sup>127</sup>

The EU ranks highest in the world for hosting 'horrific' images and videos of child sexual abuse, with 59 per cent of world CSA reports coming from EU countries.<sup>128</sup>



**of child abuse reports were traced to hosting services in EU countries**

123 European Commission, 'Questions and Answers on the Digital Services Act' (23 February 2024) <[https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_20\\_2348](https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348)> accessed 3 March 2025.

124 Article 28, Online protection of minors - the Digital Services Act (DSA), requires that online platforms accessible to minors implement appropriate and proportionate measures to ensure a high level of privacy, safety, and security for these users. Specifically, platforms must refrain from presenting advertisements based on profiling using personal data of minors., European Parliament and Council, *Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)* [2022] OJ L 277/1, Article 28.

125 5Rights Foundation, 'On the European Commission's guidelines on DSA Article 28(1)', European Commission, 'Protection of Minors – Guidelines' <[https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en)> accessed 31 October 2024.

126 CSA Centre, 'Key messages from research on the impacts of child sexual abuse' (March 2023) <<https://www.csacentre.org.uk/research-resources/key-messages/impacts-of-child-sexual-abuse/>> accessed 3 March 2025.

127 European Commission, 'EU Strategy for a More Effective Fight Against Child Sexual Abuse' COM (2020) 607 final.

128 Internet Watch Foundation, 'EU still hosts the most child sexual abuse material in the world' (26 April 2023) <<https://www.iwf.org.uk/news-media/news/eu-still-hosts-the-most-child-sexual-abuse-material-in-the-world/>> accessed 6 November 2024.

In 2023, 29,044 Irish reports contained CSA material, significantly increased from 2022 and with a troubling increase in self-generated CSA.<sup>129</sup> While children may be abused for CSAM anywhere in the world, Ireland is not immune from the production, consumption, and harm of this abuse, with 25 active cases of CSAM involving Irish children being investigated by an Garda Síochána in the first half of 2024.<sup>130</sup>

Attempts to protect children from harm and abuse by CSAM have been slow and faltering at EU level. A proposed Regulation, introduced in 2022, aims to address the increasing prevalence of CSAM online by requiring tech companies to detect, report, and remove abusive content proactively, with a particular emphasis on end-to-end encrypted environments.<sup>131</sup> The Regulation as drafted seeks to balance privacy and security, implementing stringent requirements for detection tools and transparency in data processing. Meanwhile, a complementary recast Child Sexual Abuse Directive aims to bolster Member States' legislative frameworks, encouraging more stringent definitions and penalties for CSAM-related offences while harmonising minimum

standards across the EU. It also emphasises victim-centred approaches, including better support and rehabilitation services. The combined effect of these initiatives would establish a more cohesive and robust EU-wide approach to prevent, investigate, and prosecute CSAM offences, while adapting to evolving digital technologies and legal challenges related to privacy and data protection.<sup>132</sup>

However, the CSAM Regulation and CSA Directive were not passed by the last European Parliament, the term of which ended in June 2024. While the proposal to deal with child sexual abuse material was broadly welcomed, the debate on the measure became polarised, principally on concerns of interference with data protection and privacy.<sup>133</sup>

Following the election of a new European Commission and Parliament in 2024, the CSAM Regulation may come back before the Parliament again. However, there is a real concern amongst those advocating for children and young people that their right to protection and to be free from abuse will not be prioritised. This then leaves children in Ireland, Europe, and

## 2022



**A proposed Regulation aiming to address the prevalence of CSAM online is introduced**

## 2023



**CSAM reports to Hotline.ie (Ireland) increase by 280% from 2022**

## 2024



**The CSAM Regulation and CSA Directive are not passed by the last European Parliament, the term of which ended in June 2024**

129 4,322 of the CSAM reports to Hotline.ie involved self-generated CSAM. This marks a 280 per cent increase from the previous year and highlights a significant issue in children being sexually exploited after sending images or videos. 57 per cent of the material displayed preteen children and 43 per cent were in their early teens, 97 per cent were female. See *Hotline.ie, Hotline.ie Annual Report 2023* (October 2024) 8, 14,11, 18.

130 RTÉ News, 'Over 25 children "identified as victims of online child abuse material" so far this year' (25 April 2024) <<https://www.rte.ie/news/ireland/2024/0425/1445650-policing-authority/>> accessed 4 December 2024.

131 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse' COM (2022) 209 final.

132 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, as amended by COM (2023) 94 final.

133 European Parliamentary Research Service, *EU Action Against Child Sexual Abuse Material* (Briefing, 2022) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS\\_BRI\(2022\)738224\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf)> accessed 28 October 2024.

around the world without adequate protection, and perhaps without any protection at all when a current voluntary monitoring scheme expires in April 2026.

The proposed EU Regulation to combat child sexual abuse would require online service providers to conduct risk assessments and implement measures to prevent their platforms from being used for abuse. To be effective, the Regulation must comprehensively target both known and unknown child sexual abuse material, as well as grooming. However, the European Parliament's current position restricts voluntary detection and limits detection orders to known CSAM, excluding grooming.<sup>134</sup> This approach has faced significant criticism for potentially undermining child protection online.<sup>135</sup> To address these gaps, the Regulation must explicitly include mandatory detection and reporting mechanisms for grooming and unknown CSAM, with clear accountability for platforms. In response to ongoing challenges, the European Commission has proposed extending the Interim Regulation, which currently allows for voluntary detection of CSAM, to ensure continued protection until the new Child Sexual Abuse Regulation (CSAR) framework is formally adopted.<sup>136</sup> This is a pragmatic interim approach, but the lack of baseline requirements means that approaches and standards in its application vary, which is far from ideal.

### Child Rights Impact Assessments (CRIA)

Child Rights Impact Assessments (CRIAs) are essential tools for ensuring that digital policies, platforms, and services prioritise the safety and well-being of children. As emphasised in UNCRC General Comment No. 25, States should require CRIAs to assess both potential benefits and risks to children's rights, including impacts on their privacy, freedom of expression, and protection from harm, before implementing digital initiatives.<sup>137</sup> CRIAs enable policymakers and tech companies to proactively address

children's vulnerabilities in digital spaces, fostering environments that support rather than compromise their development and rights.

Encouragingly, Ireland has committed to embedding Child Rights Impact Assessments (CRIAs) into public policy and decision-making in *Young Ireland: National Policy Framework for Children and Young People 2023-2028*.<sup>138</sup> In 2024, the Department of Children, Equality, Disability, Integration and Youth committed to developing a CRIA prototype, informed by research undertaken by the Children's Rights Alliance, the UNESCO Child and Family Research Centre, and Foróige. For Coimisiún na Meán, the use of CRIAs could ensure the systematising of children's rights within and across their functions and may also act as a blueprint for what should be required of platforms when they are undertaking CRIAs.

### Platform Accountability

The measures required to protect children and young people from online harm must extend beyond the creation of legislation and regulation to include robust implementation, as mandated by the UNCRC. Specific rights under the UNCRC obligate States to adopt comprehensive measures to safeguard children in digital environments, including the regulation of online platforms. These rights include:

- **Article 6** - The right to life, survival, and development
- **Article 19** - Protection from violence, abuse, and neglect
- **Article 34** - Protection from sexual exploitation and abuse

134 Child sexual abuse online Regulation: moving the debate forward' (5 February 2024) <<https://cdn.digitaleurope.org/uploads/2024/02/DIGITALEUROPE-CSAM-How-to-move-the-debate-forward-Feb-2024.pdf>> accessed 3 March 2025.

135 Eurochild, 'Don't look away: we must protect children from child sexual abuse online' (Eurochild, 10 May 2023) <<https://eurochild.org/news/dont-look-away-we-must-protect-children-from-child-sexual-abuse-online/>> accessed 3 March 2025.

136 European Parliament, 'Child sexual abuse online: current rules extended until April 2026' (Press Release, 10 April 2024) <<https://www.europarl.europa.eu/news/en/press-room/20240408IPR20311/child-sexual-abuse-online-current-rules-extended-until-april-2026>> accessed 3 March 2025.

137 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 38.

138 Department of Children, Equality, Disability, Integration and Youth, *Young Ireland: National Policy Framework for Children and Young People 2023-2028* (2023), s.3.3.

General Comment No. 25 further stresses the importance of holding platforms accountable for failing to meet these obligations. As regulation in this sphere is still emerging, mechanisms for ensuring accountability remain limited, underscoring the need for robust enforcement to uphold children's rights effectively.

The European Commission, in conjunction with Digital Services Coordinators in EU Member States, of which Coimisiún na Meán is one, have begun investigations under the EU Digital Services Act (DSA) into various online platforms to ensure their compliance with new regulations aimed at enhancing transparency, accountability, and safety for users across the EU.

The European Commission's investigations, particularly into Very Large Online Platforms (VLOPs) such as Meta,<sup>139</sup> X (formerly Twitter),<sup>140</sup> and Temu,<sup>141</sup> address several core DSA provisions, focusing on systemic risks, data access for researchers, advertising transparency, and manipulative design features (commonly referred to as 'dark patterns'). At the time of publication of this report, the European Commission is examining X's handling of illegal content, advertising transparency, data access, content

moderation, and potential deceptive design practices.<sup>142</sup> Meta is similarly being investigated for concerns that the systems of both Facebook and Instagram, including their algorithms, may stimulate behavioural addictions in children, as well as create so-called 'rabbit-hole effects'.<sup>143</sup> In addition, the European Commission is also concerned about the adequacy of age-assurance and verification methods put in place by Meta.<sup>144</sup> It has also initiated a formal investigation into Temu, focusing on the possible sale of illegal products and the use of manipulative design features,<sup>145</sup> such as gamification or the illusion of scarcity.<sup>146</sup>

At the same time as the European Commission investigations, but in an independent move, Coimisiún na Meán has launched a review into major platforms like TikTok, Meta, X, and YouTube, to evaluate the extent to which these platforms provide effective contact mechanisms and reporting tools for people who are trying to report illegal content on the platforms. The platforms covered in this review include some of those covered by the Online Safety Code, but it extends to others as well.<sup>147</sup> The regulator's review holds significant weight, as any

- 139 In May 2024, the Commission opened formal proceedings against Meta, the parent company of Facebook and Instagram, to evaluate potential breaches of the DSA, particularly concerning the protection of minors. The investigation centres on whether Meta's systems, including algorithms, contribute to behavioural addictions in children and create "rabbit-hole effects." Additionally, the Commission is scrutinising Meta's age-assurance and verification methods, European Commission, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (16 May 2024) <<https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-meta-under-digital-services-act-related-protection>> accessed 1 November 2024.
- 140 In December 2023, the Commission commenced formal proceedings against X to determine if the platform violated DSA obligations related to risk management, content moderation, dark patterns, advertising transparency, and data access for researchers. The investigation was prompted by concerns over X's handling of illegal content, the effectiveness of its content moderation resources, and the transparency of its advertising practices. European Commission, 'Commission opens formal proceedings against X under the Digital Services Act' (18 December 2023) <[https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_23\\_6709/IP\\_23\\_6709\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_6709/IP_23_6709_EN.pdf)> accessed 1 November 2024.
- 141 Temu is an online marketplace. In October 2024, the Commission launched an investigation into Temu, a Chinese e-commerce platform, to assess its compliance with the DSA. The probe focuses on whether Temu has effectively prevented the sale of illegal products, addressed risks related to consumer protection and public health, and complied with transparency obligations, including data access for researchers and the use of manipulative design features, POLITICO, 'EU opens probe into Chinese e-commerce platform Temu' (31 October 2024) <<https://www.politico.eu/article/eu-opens-probe-into-chinese-e-commerce-platform-temu/>> accessed 1 November 2024.
- 142 European Commission, 'Commission opens formal proceedings against X under the Digital Services Act' (18 December 2023) <[https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_23\\_6709/IP\\_23\\_6709\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_6709/IP_23_6709_EN.pdf)> accessed 1 November 2024.
- 143 European Commission, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (16 May 2024) <[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_24\\_2664](https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664)> accessed 7 November 2024.
- 144 European Commission, 'Commission sends preliminary findings to X for breach of the Digital Services Act' (European Commission, 12 July 2024) <[https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_24\\_3761/IP\\_24\\_3761\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_3761/IP_24_3761_EN.pdf)> accessed 30 October 2024.
- 145 POLITICO, 'EU opens probe into Chinese e-commerce platform Temu' (31 October 2024) <<https://www.politico.eu/article/eu-opens-probe-into-chinese-e-commerce-platform-temu/>> accessed 1 November 2024.
- 146 Michael E. Smith, 'How Temu Uses Psychological Hacks to Encourage Overspending' (Psychology Today, 4 April 2024) <<https://www.psychologytoday.com/ie/blog/the-social-consumer/202404/how-temu-uses-psychological-hacks-to-encourage-overspending>> accessed 4 March 2025.
- 147 TikTok, X, YouTube, Meta, LinkedIn, Temu, Pinterest, Shein, Etsy, Dropbox, Hostelworld and Tumblr have been issued with formal requests for information to ensure they are complying with their obligations under the EU Digital Services Act (DSA). Irish Legal News, 'Irish Regulator Probing Online Platforms Over Reporting of Illegal Content' (*Irish Legal News*, 21 February 2024) <<https://www.irishlegal.com/articles/irish-regulator-probing-online-platforms-over-reporting-of-illegal-content>> accessed 4 March 2025.

findings of non-compliance may lead to formal investigations, compliance orders, or substantial fines, underscoring Coimisiún na Meán's authority to enforce the DSA on platforms with headquarters in Ireland.<sup>148</sup>

Some platforms have made incremental changes to address child safety concerns, such as TikTok limiting push notifications for younger teens and introducing a screen-time management tool for under 18s,<sup>149</sup> and Instagram's recent introduction of private-by-default 'teen accounts' in certain regions along with enhanced parental supervision tools.<sup>150</sup> However, these measures rely heavily on users accurately reporting their age, with no proactive steps to identify and remove underage users. Additionally, the burden falls on children to manage screen time and on parents to monitor accounts, which is ineffective in situations where children may be vulnerable or lack family support, raising concerns about the adequacy of these protections.

## Safety-by-Design

The Australian eSafety Commissioner has emphasised the need for a 'Safety-by-Design' framework, recommending that tech companies adopt user-centred design principles that include real-time interventions and proactive risk assessments to minimise harm.<sup>151</sup> These frameworks emphasise that platforms should pre-emptively address risks to create safer, more responsible digital spaces.<sup>152</sup> Without stringent and robust age verification, platforms remain insufficiently equipped to protect children from harmful or illegal content, or features that may negatively affect their well-being, as they have no way of knowing whether the user is a child or not. How children and young people experience content and online features will be different from adults. What is considered harmful to a child may not be so to an adult, and vice versa. There is a significant risk that without a comprehensive

requirement for age verification, other safety-by-design and privacy-by-design measures cannot be effectively implemented as there is no way of knowing whether the user is a child thus limiting their utility in protecting children and young people online.<sup>153</sup> 5Rights Foundation has identified a number of design risks which must be included in any comprehensive response, along with actions platforms must be required to take to mitigate these risks before they can be truly considered as 'Safety-by-Design' or 'Privacy-by-Design'. These include, although are not limited to:



- **Infinite scroll and autoplay features**  
Regulation must require that these features be disabled by default for child and young users
- **In-app purchases or platform features**  
Regulation must require that these features be disabled by default for child and young users
- **Connections such as 'friends' or chat functions with users unknown to the child or young user**  
Regulation must require that unknown contacts be blocked by default for child and young users
- **Anonymous users being able to contact, connect, interact, or communicate with a child or young user**  
Regulation must require that anonymous users be blocked by default for young users
- **Live streaming and sharing images of children and young people**  
Regulation must require that images, including detecting nudity in any images/videos to prevent upload and sharing, and live streaming of or by child and young users not be visible to any person that is unknown to the child, including anonymous users

148 Coimisiún na Meán, 'Coimisiún na Meán opens review of online platforms' compliance with EU Digital Services Act' (12 September 2024) <<https://www.cnam.ie/coimisiun-na-mean-opens-review-of-online-platforms-compliance-with-eu-digital-services-act/>> accessed 1 November 2024.

149 TikTok, 'New Features to Support Screen Time Management for Teens' (1 March 2023) <<https://www.tiktok.com/screentime-management-teens>> accessed 4 November 2024; TikTok, 'TikTok Introduces Changes to Push Notifications for Younger Teens' (1 March 2023) <<https://www.tiktok.com/push-notifications-teens>> accessed 4 November 2024.

150 Instagram, 'Instagram Introduces Teen Accounts with Enhanced Privacy and Parental Controls' (14 September 2024) <<https://about.instagram.com/teen-accounts>> accessed 4 November 2024.

151 Australian eSafety Commissioner, Safety by Design: Overview (eSafety Commissioner 2020) <<https://www.esafety.gov.au>> accessed 29 September 2024.

152 *ibid.*

153 5Rights Foundation, *But How Do They Know It is a Child?* (2024) <[https://5rightsfoundation.com/wp-content/uploads/2024/09/But\\_How\\_Do\\_They\\_Know\\_It\\_is\\_a\\_Child-1.pdf](https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf)> accessed 30 September 2024.

- **Excessive notifications, push notifications, and unlimited time usage**

Regulation must require that out-of-app notifications and push notifications be switched off by default for child and young users

The guidelines must also require time limits and regular breaks as mandatory for child and young person's accounts

- **Public displays of popularity signals such as 'likes' or numbers of friends**

Regulation must require that indicators of popularity be made completely private to all users except the child or young user themselves

- **Recommender systems and algorithms based on personal data and user behaviour**

Regulation must require that recommender systems and algorithmic profiling be disabled by default for child and young users

- **Tagging or identifying people in photos, videos, live streams, or chats**

Regulation must require that that all 'tagging' in photos, videos, live streams, or chat features be disabled by default for child and young users

- **Live streaming**

Regulation must require that live streaming be disabled by default for child and young users. This must also include disabling the ability to watch live streams by child and young users

- **Profiling and data gathering**

Regulation must require that all profiling and data gathering be disabled by default for child and young users.<sup>154</sup>



## Remedies for Rights Violations

The UN Committee on the Rights of the Child has identified that children can face particular challenges accessing justice relating to the digital environment for a range of reasons. Such challenges may include a lack of adequate systems and legislation, difficulty in obtaining evidence or naming perpetrators, or because children, their parents, and caregivers lack knowledge of their rights.<sup>155</sup>

It highlights the need for complaint and reporting systems that are accessible, fair, child friendly, safe, appropriate, and provide effective remedies and redress to someone who has been harmed.<sup>156</sup> If well structured, such complaints and reports systems are not only valuable to the person who makes a report of harm and gets redress, but they also help to build trust and accountability within organisations that have such systems in place. They also build better structures and systems throughout whole industries and institutions.<sup>157</sup> Either directly or through the regulator, the State must ensure that systems and structures for complaints recognises the rights of users. Currently, the methods available are not comprehensive enough to ensure those rights.

A complaint or report may relate to matters which are illegal or harmful, disseminating certain information relating to terrorism, child sexual abuse, illegal hate speech, or infringements of consumer protection laws, self-harm or suicide encouragement, or violent or graphic content.<sup>158</sup> The report and complaint systems which currently exist do not make it easy for a person who is harmed to complain and get redress as there are different avenues of complaint, and further, not all the complaints systems that are needed are yet in place.

- 154 5Rights, Web Resource, 'Risky by Deign', <<https://www.riskyby.design/friend-suggestions>> accessed 27 September 2024; 5Rights, 'Pathways: How digital design puts children at risk' (2021) <<https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf>> accessed 27 September 2024 ; American Psychological Association, 'Potential risks of content, features, and functions: The science of how social media affects youth' (2024) <<https://www.apa.org/topics/social-media-internet/psychological-science-behind-youth-social-media.pdf>> accessed 27 September 2024.
- 155 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 43.
- 156 *ibid*, para 43-44. Children and young people must also have a right to an effective remedy to justice under the European Convention of Human Rights, and a child friendly remedy as outlined in the Council of Europe Guidelines on Child Friendly Justice, see 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.
- 157 Article 8 UDHR. Ombudsman Model Complaints system <<https://assets.ombudsman.ie/media/285094/27141f4a-453e-4713-8abe-9fbe409e876a.pdf>> accessed 19 November 2024.
- 158 For what constitutes illegal content under the Dsa see, European Commission, 'Commission Recommendation (EU) 2018/334 of 1 March 2018 on Measures to Effectively Tackle Illegal Content Online' [2018] OJ L63/50. For what constitutes harmful content under the Online Safety and Media Regulation Act see, section 139A(1).



For content that a child or their caregiver believes is illegal, the right continues to exist to make a complaint to An Garda Síochána. That necessarily requires the child or their caregivers to report a criminal complaint. However, if a child is not ready or does not wish to make a criminal complaint, or in addition, seeks the take down of material from a platform as a remedy, then they must first apply to the platform where the harmful or illegal material appears. The legislation requires that children are protected, and as part of that, they need to have an effective remedy provided by the platforms. General Comment No. 25, the Digital Safety Act (DSA), and the Online Safety Code<sup>159</sup> all require that platforms have accessible and effective mechanisms to ensure that complaints by children or their caregivers are dealt with promptly and effectively.

There is no standard method of complaint, and each platform will devise its own system. This immediately creates a lack of accessibility given that multiple platforms may host the same or similar abusive material, and the complainant will be expected to know and be familiar with each platform's systems. In addition, a complainant seeking a speedy and effective remedy for abusive, harmful, illegal material online which is having a harmful impact on them is then required to seek out and understand platform's systems at a time when they may be traumatised, frightened, and pressurised by the complained of material.

No system of aid or assistance is provided by the regulator or the State to someone who contacts a platform directly who wants to make a complaint or a request to have material removed. A newly created process of 'Trusted Flagger' will allow specific authorised organisations to report

harmful or illegal online content with priority access to the relevant platform's complaint mechanism.<sup>160</sup> These Trusted Flaggers, approved for their expertise in areas like child protection and public safety, receive privileged reporting rights to expedite content removal. To our knowledge, no organisation has been formally designated as a Trusted Flagger to date.<sup>161</sup> Meanwhile several organisations have informal arrangements with various platforms, but these are subject to the willingness of the platforms to engage with advocacy associations.

The DSA, which creates the concept of Trusted Flaggers, also provides for authorised out-of-court dispute settlement (ODS) bodies, such as the Appeals Centre Europe,<sup>162</sup> to resolve disputes relating to decisions of online platforms, including complaints that have not been resolved by means of the internal complaint-handling system of an online platform. The Appeals Centre Europe, based in Dublin, was publicly announced in October 2024 as one such centre.<sup>163</sup> The decisions of ODS bodies are not binding.<sup>164</sup> This may in time contribute to platform accountability for widespread problems without individual complaints but meanwhile, it is of little benefit to a user who needs redress or a remedy in a timely and effective way.<sup>165</sup>

The current system of complaint is mainly an internal one where the platform which hosts the illegal or harmful content is the principal adjudicator. This is particularly so for 'harmful' content which is mainly regulated by the Online Safety Code, rather than the DSA but where even a report to Coimisiún na Meán does not result in moderation of any dispute.<sup>166</sup> For this reason, the underlying legislation has provided for a new individual complaints mechanism to be set up which will allow for individual complaints

159 Part A Section 10.6(d), (e),(i) and in Part B Section 16.1, 16.2, 16.3, 16.4, Coimisiún na Meán, Online Safety Code (October 2024), <[https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean\\_Online-Safety-Code.pdf](https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf)> accessed 18 November 2024.

160 Article 22 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

161 Coimisiún na Meán, 'Trusted Flaggers under the Digital Services Act' (Coimisiún na Meán, 2024) <<https://www.cnam.ie/coimisiun-na-mean-outlines-how-interested-entities-can-apply-for-trusted-flagger-status/>> accessed 31 October 2024.

162 Appeals Centre Europe, 'Rules of Procedure' (2024), < [https://www.appealscentre.eu/rules-of-procedure/#:~:text=Appeals%20Centre%20Europe%20\(Appeals%20Centre,known%20as%20the%20Digital%20Services](https://www.appealscentre.eu/rules-of-procedure/#:~:text=Appeals%20Centre%20Europe%20(Appeals%20Centre,known%20as%20the%20Digital%20Services)> accessed 03 March 2025.

163 Jenny Darmody, 'Ireland has a new dispute body for social media users' (Silicon Republic, 8 October 2024) <<https://www.siliconrepublic.com/business/social-media-dispute-body-appeals-centre-europe/>> accessed 7 November 2024; Mathieu Pollet, 'EU Tech Bastion Ireland Brings in New Rules to Crack Down on X, TikTok' Politico (22 October 2024) <<https://www.politico.eu/>> accessed 31 October 2024; Scout Mitchell, 'Moderation: In Ireland, a Center for Making Complaints' Swords Today (10 October 2024) <<https://swordstoday.ie/moderation-in-ireland-a-center-for-making-complaints/>> accessed 31 October 2024.

164 Coimisiún na Meán, 'Digital Services Act – Guidance for Industry' (Coimisiún na Meán, 2024) <<https://www.cnam.ie/dsaindustry/>> accessed 13 November 2024.

165 Articles 33 and 34 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

166 Coimisiún na Meán Webpage, 'Online Complaints' (Coimisiún na Meán, 2024) <<https://www.cnam.ie/onlinecomplaints/>> accessed 13 November 2024.

to the Online Safety Commissioner.<sup>167</sup> This new system has not yet been set up. In line with recommendations from the Expert Group on the individual complaints' mechanism,<sup>168</sup> Coimisiún na Meán is following advice that it should first develop online safety codes regarding standards in complaints handling and monitor compliance over a twelve-month period to assess which areas need most urgently to be tackled via the individual complaint's mechanism.<sup>169</sup>

This does not constitute an effective system of access to justice for users, including children and young people, as it places the burden on them to navigate complex, platform-controlled processes with no guaranteed resolution, leaving them vulnerable to prolonged exposure to harmful content and without a clear, independent route to enforce their rights.

Coimisiún na Meán has established a 'Contact Centre'.<sup>170</sup> This can receive reports from users of online services who believe that a provider of an online service has not complied with its obligations under the DSA.<sup>171</sup> This relates principally to illegal content on the platforms. Their role is to ensure platforms have a complaint mechanism in place and are operating them diligently.<sup>172</sup> It is not to moderate complaints. It therefore does not provide an alternative to the platforms, nor an appeal from their decisions.

Ensuring children's right to an effective and child friendly remedy is critical to safeguarding their well-being in digital spaces. While mechanisms like Coimisiún na Meán's Contact Centre and the EU's complaint provision<sup>173</sup> mark essential progress, further enhancements in accessibility and efficiency are needed. A robust, responsive

system for addressing children's online safety concerns remains vital for upholding their rights in Ireland and beyond.

Offenders who post online abuse or harmful content can be restricted under the new Online Safety Code but a single instance of abuse or harmful content, no matter how serious the content or the impact, will not trigger sanctions.<sup>174</sup> To ensure a safe and supportive environment for children and young people, platforms must implement clear measures to address 'single serious incidents' that pose harm, or risk of harm, to children and not require a pattern or accumulation of harms before action is taken. This would also ensure there is an obligation for swift and decisive action to be taken to remove harmful content. This must be in addition to suspending accounts that frequently breach terms of service. Platforms must be required to immediately remove content that involves or poses serious harm to children.



167 Online Safety and Media Regulation Act 2022, s 139R, s 45, Part 11, Ch 4.

168 Expert Group on an Individual Complaints Mechanism, *Report of the Expert Group on an Individual Complaints Mechanism* (Department of Children, Equality, Disability, Integration and Youth, May 2022).

169 Coimisiún na Meán, 'Coimisiún na Meán holds first meeting of Youth Advisory Committee' 19 December 2023, <<https://bit.ly/ws/3aPiB>> accessed 25 January 2024

170 TechCentral.ie, 'Coimisiún na Meán opens contact centre providing information on Digital Services Act enforcement' (TechCentral.ie, 19 February 2024) <<https://www.techcentral.ie/coimisiun-na-mean-opens-contact-centre-providing-information-on-digital-services-act-enforcement/>> accessed 13 November 2024. Coimisiún na Meán, Online Complaints (Coimisiún na Meán) <<https://www.cnam.ie/onlinecomplaints/>> accessed 31 October 2024.

171 Coimisiún na Meán, Online Complaints (Coimisiún na Meán) <<https://www.cnam.ie/onlinecomplaints/>> accessed 31 October 2024.

172 *ibid.*

173 Internal Complaint-Handling Systems: Article 20 of the Digital Services Act (DSA) requires online platforms to implement effective internal systems that allow users to lodge complaints against certain decisions made by the platform, such as the removal of content or suspension of accounts. Out-of-Court Dispute Settlement: Article 21 provides for the establishment of certified out-of-court dispute settlement bodies. These bodies offer an alternative means for users to resolve disputes with platforms regarding content moderation decisions. Trusted Flaggers: Article 22 introduces the concept of "Trusted Flaggers," entities recognized for their expertise in identifying illegal content. Notifications from Trusted Flaggers are to be prioritized by platforms. European Union, *Digital Services Act*, Articles 20-22.

174 Part B of the Online Safety Code only requires that platform providers suspend, after prior warning and for a reasonable period, services to users who 'frequently' infringe the terms and conditions, see Coimisiún na Meán, Online Safety Code (October 2024) <[https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean\\_Online-Safety-Code.pdf](https://www.cnam.ie/wp-content/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf)> accessed 31 October 2024, sections 12.6, 13.6.

## Enforcing Regulation on the Online Industry: Recommendations

- Coimisiún na Meán should establish and operate an effective and accessible individual public complaints mechanism where end-user rights and protections are fully vindicated, and complaints made by children or involving a child are given priority. The Coimisiún must also:
  - Designate trusted flaggers to address children’s online safety concerns;
  - Require platforms to prioritise complaints made by children, or involving a child;
  - Ensure the Appeals Centre Europe guarantee children timely and appropriate remedies;
  - Immediately act on all ‘single serious infringements’ where there is a potential risk of harm to a child.
- Coimisiún na Meán and the European Commission must strengthen oversight of platform compliance with the Digital Services Act. They must ensure accountability mechanisms are effective and child-centred. These must include safety-by-design, transparency, privacy and algorithms.
- The Government must lead reform of EU laws that combat the production, hosting, access and use of child sexual abuse material (CSAM). The Government must ensure these laws properly address grooming, encryption, detection and secure storage of both new and existing CSAM.
- Child Rights Impact Assessments (CRIAs) could be made mandatory for platform policies to proactively mitigate risks against children and young people and to ensure a child-centred approach. CRIAs must be fully integrated into the operations of Coimisiún na Meán.

## Section 3

# Education and prevention against harm online



## SECTION 3: EDUCATION AND PREVENTION AGAINST HARM ONLINE

The UN Convention on the Rights of the Child affirms children’s rights to:

- Freedom of Expression (Article 13);
- Freedom of Thought, Conscience, and Religion (Article 14);
- Freedom of Association and Assembly (Article 15);
- Access to Information (Article 17), and;
- Be protected from harm (Article 19).

In alignment with these rights and with General Comment No. 25 on Children’s Rights in the Digital Environment, the State holds a crucial responsibility to ensure that children, parents, caregivers, educators, and all those who interact with children are fully prepared to navigate the online world safely and responsibly.<sup>175</sup>

Integrating digital literacy into the school curriculum and other education settings is critical to preparing children and young people for safe, informed, and empowered digital participation.<sup>176</sup> Through its General Comment No. 25, the UN Committee on the Rights of the Child emphasises the importance of digital literacy, urging States to make it a core part of education from preschool through all school levels, with pedagogies assessed on their outcomes.<sup>177</sup>

The Committee also highlights that children should develop an understanding of digital infrastructure, persuasive tactics, automated processing, and data surveillance, stressing the need for teacher training on these topics.<sup>178</sup> These efforts should also extend to resources for parents and caregivers, enabling them to actively support children’s online experiences within a structured framework that aligns with children’s rights to safety and access to information.<sup>179</sup>

Children and young people must be equipped with strategies to prevent and mitigate discrimination and harm. They must be prepared to navigate complex digital environments, understanding the potential dangers related to online content, contact conduct such as misinformation and disinformation, non-consensual sharing of images, pornography, cyberaggression, exploitation, targeted advertising, the misuse of personal data, and the gender-related digital divide for girls.<sup>180</sup>

Various definitions of what constitutes digital literacies have emerged. UNESCO describes it as the ability to safely and effectively access, manage, understand, integrate, communicate, evaluate, and create information using digital technologies, particularly for employment, decent work, and entrepreneurship. This definition encompasses related concepts such as computer literacy, ICT literacy, information literacy, and media literacy.<sup>181</sup> The European Commission uses the term ‘digital competence’ to highlight the confident, critical, and responsible use of digital technologies for learning, work, and participation in society. It includes skills such as information and data literacy, communication, collaboration, media literacy, content creation including programming, digital safety covering cybersecurity and well-being, intellectual property awareness, problem-solving, and critical thinking.<sup>182</sup>

### National Strategies

The National Council for Curriculum and Assessment (NCCA) outlines the integration of digital technology into Ireland’s primary education curriculum, framing digital learning as a ‘suitcase’ concept that can be unpacked in various ways to meet diverse learning needs.<sup>183</sup>

175 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children’s rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), paras 29–32, 36, and 75–78.

176 OECD, *Empowering Young Children in the Digital Age, Starting Strong*, < <https://doi.org/10.1787/50967622-en> > accessed 4 March 2025.

177 United Nations 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 104.

178 *ibid*, para 105.

179 *ibid*, para 84.

180 *ibid*, paras, 54, 81, 104.

181 UNESCO, *Global Education Monitoring Report: Migration, Displacement and Education, Building Bridges, Not Walls* (UNESCO 2018).

182 European Council, Recommendation of 22 May 2018 on Key Competences for Lifelong Learning, (2018) ST/9009/2018/INIT, OJ C 189, 4.6.2018, 1–13.

183 NCCA, *Digital Technology: Being a Digital Learner* (NCCA 2020) 7.

It highlights the importance of fostering key competencies such as critical thinking, creativity, and responsible digital engagement while aligning educational policies with the demands of a technology-driven world.<sup>184</sup> The NCCA has emphasised that being digital is not an 'add-on' but an integral part of what it means to be a learner situated at the very core of the learning experience.<sup>185</sup>

These varying definitions highlight the evolving and multifaceted nature of digital literacy, involving several skills but overall underscoring its critical role in empowering individuals to thrive and recognise their rights in a rapidly advancing digital world.<sup>186</sup>

The Department of Education has developed *Ireland's Literacy, Numeracy and Digital Literacy Strategy 2024-2033: Every Learner from Birth to Young Adulthood* which aims to promote essential digital literacy skills across all educational stages, from early learning and care to post-primary education.<sup>187</sup> This Strategy outlines objectives under five key Pillars, including:

- Enabling parents and communities to support learners' literacy, numeracy, and digital literacy;
- Supporting the professional practice of early years educators, childminders, and teachers;
- Supporting leadership in early learning and care, and in the school system;
- Improving the learner experience through curriculum, pedagogy, and assessment;
- Supporting diverse learners to achieve their potential.<sup>188</sup>

*The Implementation Plan* included with the *Strategy* includes high-level objectives and covers the period 2024-2028. It adopts an integrated approach to digital literacy, embedding it within broader objectives that also encompass numeracy and traditional literacy. This is intended to ensure digital literacy is addressed throughout the educational framework rather than foresee it as a standalone module or subject.<sup>189</sup> This is with the exception of the general obligation to 'promote online safety and digital citizenship to enable parents to support their children in the autonomous, effective and safe use of the online world'.<sup>190</sup> Key stakeholders for this action are named as Webwise and Tusla – the Child and Family Agency. The plan highlights the importance of online safety, educator training, and equipping learners with the skills for confident and ethical use of digital technologies.<sup>191</sup> The recently updated Social, Personal and Health Education (SPHE) curriculum now addresses important topics such as cyberbullying, the non-consensual sharing of images, and digital wellbeing.<sup>192</sup>

Currently, only the post-primary Junior Cycle curriculum offers digital media studies through a digital media course, in which the stated design objective is to equip students with the skills necessary to navigate and engage with digital technologies effectively.<sup>193</sup> This course is optional and is not exclusively focused on digital literacy or online safety. As noted above, in regard to the primary curriculum, the NCCA emphasises key approaches to integrating digital technology across the curriculum.<sup>194</sup> The importance of aligning educational policies with classroom practices is highlighted, particularly through frameworks such as the Digital Strategy

---

184 *ibid.*

185 *ibid.*

186 *ibid.*

187 Department of Education, *Ireland's Literacy, Numeracy and Digital Literacy Strategy 2024-2033: Every Learner from Birth to Young Adulthood* (Department of Education, 2023).

188 *ibid.*

189 *ibid.*

190 *ibid.*, Action 1.1.1b.

191 *ibid.*, Action 1.1.1b to Promote online safety and digital citizenship to enable parents to support their children in the autonomous, effective and safe use of the online world. Action 1.3.7 to support youth services in training for spotting online misinformation, Action 2.1.1 to enhance educators' literacy skills through professional learning communities, Action 2.1.6 to provide flexible training to boost digital literacy in educators, Action 4.3.1 to carry out a public consultation and develop a national policy statement on the use of digital technologies and digital learning in Early Learning and Care.

192 National Council for Curriculum and Assessment, *Junior Cycle Social, Personal and Health Education (SPHE) Short Course Specification 2023* (NCCA, 2023), sections 2.7, 2.8, 3.10, 4.5, 4.6 and 4.7.

193 National Council for Curriculum and Assessment, *Junior Cycle Short Course: Digital Media Literacy* (NCCA, 2016).

194 NCCA, *Digital Technology: Being a Digital Learner* (NCCA 2020).

for Schools, the Digital Learning Framework, and the Primary Curriculum Framework.<sup>195</sup> The NCCA also highlights the importance of a coherent approach between policy and practice to ensure that digital technology is embedded effectively, rather than treated as an optional extra.<sup>196</sup> It underscores the development of key competencies, advocating for digital literacy to be a fundamental skill that enables students to become curious, creative, confident, and critical users of digital technology.<sup>197</sup>

While the *Strategy* and the *Implementation Plan* include reference to online safety, neither require nor foresee online safety as being included as a specific aspect of the education curriculum. Instead, the focus in the *Implementation Plan* is on supporting parents to protect their children online. This is a missed opportunity to ensure that the skills and knowledge necessary to educate and protect children from online harm is fully embedded in the curriculum. Other Government policies have identified online safety and digital literacy as important,<sup>198</sup> the *Online Safety Action Plan 2018-2019* was the first and only action plan for online safety published by the State to date.<sup>199</sup> While the *Online Safety Action Plan* provided an initial framework to address online risks, particularly among children, the plan expired in 2019.<sup>200</sup>

### Coimisiún na Meán Action on Digital Literacy

Under the *Online Safety and Media Regulation Act (OSMR)*, Coimisiún na Meán is authorised to promote or endorse educational and training initiatives, and activities to promote public awareness, knowledge, and understanding in relation to matters connected to its functions.<sup>201</sup> In its first *Online Safety Code*, Coimisiún na Meán

specifically requires that each of the designated platform providers develop and publish an action plan detailing measures to promote media literacy, such to be updated annually to reflect ongoing efforts and improvements.<sup>202</sup>

In parallel to this obligation on the platforms, Coimisiún na Meán itself has begun to create educational resources on online safety for students, teachers, and parents. For students, resources are designed to raise awareness of children's rights online and promote safe digital interactions. The resources for teachers and educators provide them with materials to allow them to integrate online safety into their curriculum, enabling them to address issues such as cyberbullying and privacy. Resources for parents focus on helping them understand and manage online safety risks, providing guidance on protecting their children's digital well-being.<sup>203</sup> Importantly, *CyberSafeKids' 2023 Trends and Usage Report* shows that while online safety is a significant concern in schools, 45 per cent of teachers surveyed feel they do not have sufficient knowledge or skills to effectively deliver online safety educational messages.<sup>204</sup> This underscores the need for dedicated training and the integration of digital literacy into teacher education.

### Online Safety Initiatives

As part of Budget 2025, €9 million of ringfenced funding was allocated to the Department of Education to provide secondary schools with lockable phone pouches, with the aim of creating smartphone-free environments during school hours. This initiative, part of the 'Keeping Childhood Smartphone Free' programme,<sup>205</sup> was stated to enhance students' mental health

195 *ibid*, 7, 13-18.

196 *ibid*, 13, 15, 17.

197 *ibid*, 16.

198 For example, *Young Ireland National Policy Framework for Children and Young People 2023-2028* identifies online safety for young people as a central concern, Department of Children, Equality, Disability, Integration and Youth, *Young Ireland: National Policy Framework for Children and Young People 2023-2028* (Government of Ireland, 2023) 27 and 108.

199 Government of Ireland, *Action Plan for Online Safety 2018-2019* (Government of Ireland, 2018).

200 The *Action Plan for Online Safety 2018-2019* was Ireland's inaugural initiative to enhance online safety, particularly for children. A *Progress Report* covering the first six months (July to December 2018) indicated that 22 of the 26 constituent actions due by the end of 2018 were achieved, with the remainder showing significant progress. However, comprehensive evaluations of the plan's overall success are not readily available in the provided sources. The plan acknowledged that further actions would be required beyond its 18-month scope to continue addressing online safety challenges, Government of Ireland, *Progress Report on the Action Plan for Online Safety 2018-2019* (2019).

201 *Online Safety and Media Regulation Act 2022*, s8.

202 Coimisiún na Meán, *Online Safety Code* (2024) s 4.1, paras 10.6(j) and 17.1.

203 Coimisiún na Meán, *Online Safety Resources* <<https://www.cnam.ie/online-safety/>> accessed 14 November 2024.

204 CyberSafeKids, *Trends & Usage Report 2023* (September 2023)

205 Government of Ireland, 'Keeping Childhood Smartphone Free' (7 November 2023) <<https://www.gov.ie/en/publication/ece25-keeping-childhood-smartphone-free/>> accessed 03 March 2025.

and learning outcomes by reducing distractions associated with mobile phone use.<sup>206</sup> The plan has faced criticism from opposition parties, and teachers' and students' unions, who argue that the funds could be better utilised to address pressing issues such as teacher recruitment and retention.<sup>207</sup> The proposal aims to build a culture where children and young people achieve a balance between access to digital technology on the one hand and a learning environment that is free of unnecessary distractions on the other.

Separately, in September 2024, the Minister for Health established an Online Health Taskforce to develop a public health response to harms caused to children and young people by certain types of online activity. Chaired by former Senator and child rights advocate Jillian van Turnhout, with membership from a number of experts groups including young people, and supported by a secretariat within the Department of Health, it is tasked with identifying the range of harms which impact public health, gaps in necessary initiatives and supports, and with producing a report with recommended responses to address these harms within 12 months.<sup>208</sup>

In September 2024, Taoiseach Simon Harris chaired an Online Safety Summit of state actors including an Garda Síochána, regulators, and key department officials, to ensure a collective focus across Government on effective implementation of the newly established *Online Safety Framework*.<sup>209</sup> This was followed by a second Summit meeting of the Taoiseach and other Ministers with child rights advocates, online rights advocates, and academics in October 2024, immediately ahead of the dissolution of the Dáil and the calling of a general election.

While progress has begun in integrating digital technologies into teaching and learning through the inclusion of modules in SPHE and Relationships and Sexuality Education (RSE),

the *Literacy, Numeracy and Digital Literacy Strategy*, and resources by Coimisiún na Meán, the approach to digital literacy education remains uneven, not fully inclusive, and may leave some children and young people behind. Current efforts to equip children and young people with the skills to navigate digital spaces, such as identifying and reporting digital threats like child sexual abuse material (CSAM), harmful communications, online harassment, AI generated harms, and grooming, are not yet sufficiently comprehensive or uniformly implemented. There is also insufficient information about Irish criminal offences, such as CSAM, harmful communications, online stalking, non-consensual sharing of intimate images, and sexual exploitation within existing digital literacy programmes. Including these topics could be vital in empowering children to recognise and report illegal behaviour effectively.

A unified and inclusive strategy for digital literacy education is essential. This approach should ensure that all children, including those with disabilities, from minority backgrounds, or economically disadvantaged, can access tailored information and education that meets their diverse needs. Information and education programmes must incorporate regular evaluations, including feedback from children and educators, to measure their reach, relevance, and impact. These assessments would help identify barriers to participation and refine initiatives to ensure they are accessible and relevant. Additionally, teachers and educators must receive appropriate levels of training, not just resources, to ensure they feel confident in delivering online safety messages to children and young people. Research indicates this is not the case for many teachers survey by CyberSafeKids, which underscores the need for structured training and support.<sup>210</sup>

206 Department of Education, 'Ministers Foley, Naughton and Byrne Announce Details of Almost €12 Billion Education Funding in Budget 2025' (Press Release, 2 October 2024) <<https://www.gov.ie/en/press-release/519e2-ministers-foley-naughton-and-byrne-announce-details-of-almost-12-billion-education-funding-in-budget-2025/>> accessed 4 November 2024.

207 Joan O'Sullivan, 'Minister Defends €9m Budget Spending on Phone Storage' (RTÉ News, 2 October 2024) <<https://www.rte.ie/news/2024/1002/1473111-school-smartphone/>> accessed 4 November 2024; 'Sinn Fein Calls for Immediate Withdrawal of €9m Phone Pouch Plan' (RTÉ News, 3 October 2024) <<https://www.rte.ie/news/education/2024/1003/1473372-phone-pouches/>> accessed 4 November 2024; Irish Second-Level Students' Union, 'ISSU Criticises the Allocation of Nine Million Euro to Phone Pouches in Secondary Schools' University Times (Dublin, 10 October 2024) <<https://universitytimes.ie/2024/10/issu-criticises-the-allocation-of-nine-million-euro-to-phone-pouches-in-secondary-schools/>> accessed 4 November 2024.

208 Government of Ireland, 'Online Health Taskforce' <<https://www.gov.ie/en/publication/4d506-online-health-taskforce/>> accessed 4 November 2024.

209 Department of the Taoiseach, 'Taoiseach to chair Online Safety Summit' (18 September 2024) <<https://www.gov.ie/en/press-release/9a6df-taoiseach-to-chair-online-safety-summit/>> accessed 20 March 2025.

210 CyberSafeKids, *Trends & Usage Report 2023* (September 2023).



By embedding these principles into educational policies, the State can fulfil its obligations under the UNCRC and General Comment No. 25, ensuring a safer digital experience for all children. These initiatives will equip children, parents, caregivers, and educators with the knowledge and confidence to support children's rights in digital spaces while fostering resilience and safety.

## Educational Technology (EdTech)

The Department of Education's *Digital Strategy to 2027* has as its vision to 'empower schools to harness the opportunities of digital transformation to build digital competence and an effective digital education ecosystem so as to develop competent, critically engaged, active learners while supporting them to reach their potential and participate fully as global citizens in a digital world'. It specifies that, as far as possible in the Irish context, it aligns with the EU's *Digital Education Action Plan (2021-2027): Resetting Education and Training for the Digital Age* to offer high quality, inclusive, and accessible digital education.<sup>211</sup>

Learning with technology, called digital learning, is about using digital technologies and tools in a variety of ways, whether as a group or individual, in the classroom, at home, or in other settings.<sup>212</sup> This type of learning brings many advantages including flexibility, capacity to learn remotely, and personalised learning for those for whom mainstream learning is inaccessible. In line with the general digital environment, the number of

online learning platforms and opportunities has grown exponentially in recent years.<sup>213</sup> These may specialise in a particular form of training, may run alternative school programmes, and on some occasions, will combine with not-for-profit organisations to supply funding and technical resources to children in schools or other places where children learn and develop.

However, in addition to offering opportunities, EdTech may also pose risks to children. Many educational applications collect data from young users, often without providing adequate privacy protections. In some cases, these apps may engage in marketing practices that are not appropriate for children, promoting products or services that are unsuitable for their age group.<sup>214</sup> While these platforms may not constitute a Very Large Online Platform (VLOP) or Very Large Online Search Engine (VLOSE), the risks they pose are significant and warrant attention from regulators as well as from those who set state standards in education. There is also mixed evidence as to whether the use of these technologies improve educational outcomes for children and young people.<sup>215</sup>

A 2022 global investigation by Human Rights Watch which reviewed 165 EdTech products, found that 89 per cent engaged in data practices that put children's rights at risk, undermined them, or actively violated them.<sup>216</sup> Companies monitored children without their consent and knowledge, harvested data on what they do, who they are, where they live or study, and who their family and friends

- 211 Department of Education, *Digital Strategy to 2027* (DE 2022) 11. Other strategies include 2022- 2026 STEM Education Policy; Technology 2022 Ireland's Third ICT Action Plan; 2021-2025 Action Plan for Apprenticeship; Skillnet Ireland Programmes; and eCollege, the online learning platform, which offers free online courses in areas such as computer programming, web and graphic design. <https://digital-skills-jobs.europa.eu/en/latest/briefs/ireland-snapshot-digital-skills>. Accessed 22 November 2024.
- 212 SIRO, 'The Future of Digital Learning Looks Bright in Ireland' (23 September 2022) <<https://siro.ie/news-and-insights/the-future-of-digital-learning-looks-bright-in-ireland/>> accessed 22 November 2024.
- 213 Platform such as Google Classroom, Microsoft Teams, and Class Dojo are increasingly used. Department of Education and Skills, *Digital Learning 2020: Reporting on practice in Early Learning and Care, Primary and Post-Primary Contexts* (2020) 26.
- 214 Zhao F, Egelman S, Weeks HM, Kaciroti N, Miller AL, Radesky JS, 'Data Collection Practices of Mobile Applications Played by Preschool-Aged Children' (2020) *JAMA Pediatrics* 174(12): e203345. doi:10.1001/jamapediatrics.2020.3345. <[https://www.researchgate.net/publication/344204919\\_Data\\_Collection\\_Practices\\_of\\_Mobile\\_Applications\\_Played\\_by\\_Preschool-Aged\\_Children](https://www.researchgate.net/publication/344204919_Data_Collection_Practices_of_Mobile_Applications_Played_by_Preschool-Aged_Children)> accessed 20 March 2025.
- 215 OECD *Students, Computers and Learning: Making the Connection*, (2015) <<https://doi.org/10.1787/9789264239555-en>> accessed 20 March 2025. There is also evidence suggesting that EdTech may in fact widen rather than bridge socioeconomic divides, see Warschauer, M., Knobel, M., & Stone, L. (2004). *Technology and Equity in Schooling: Deconstructing the Digital Divide*. *Educational Policy*, 18(4), 562-588 <<https://doi.org/10.1177/0895904804266469>> accessed 20 March 2025. Ahn J, 'Exploring the Negative and Gap-Widening Effects of EdTech on Young Children's Learning Achievement: Evidence from a Longitudinal Dataset of Children in American K-3 Classrooms' (2022) 19(9) *International Journal of Environmental Research and Public Health* 5430 <<https://www.mdpi.com/1660-4601/19/9/5430>> accessed 6 December 2024. 2024. Livingstone S, 'Critical Reflections on the Benefits of ICT in Education' (2012) <<https://eprints.lse.ac.uk/42947/>> accessed 6 December 2024.
- 216 Han HJ, 'How Dare They Peep into My Private Life?': Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic' (Human Rights Watch, 2022) <<https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>> accessed 20 March 2025.

are.<sup>217</sup> The majority of the learning platforms sent or allowed access to children's data to advertising technology (AdTech) companies, many of which belong to whole supply chains owned by powerful companies like Amazon, Meta, Google, and Microsoft.<sup>218</sup> As with other platforms, safety, privacy, and data protection are key concerns, especially when it comes to children, as educational applications may exploit children's data for commercial purposes without sufficient safeguards.<sup>219</sup> In Australia, the eSafety Commissioner has the power under the Enhancing Online Safety Act 2015 'to support, encourage, conduct, accredit and evaluate educational, promotional and community awareness programs that are relevant to online safety for Australians'.<sup>220</sup> As part of this work, they publish a list of trusted providers of online safety education on their website called the Trusted eSafety Provider Program. This is designed to give schools confidence that the external online safety provider they engage meets the eSafety Commissioner's online safety education standards.<sup>221</sup>

To ensure EdTech supports rather than undermines children's rights, it is essential to establish clear regulatory standards, enforce privacy protections, and equip educators with the necessary codes of conduct, guidelines, and knowledge to safely and effectively integrate these technologies.

## Empowering Children and Young People in the Digital World

Under the United Nations Convention on the Rights of the Child (UNCRC) and further elaborated in General Comment No. 25, children's rights to association, freedom of thought, and access to reliable information must be upheld and protected within digital environments.<sup>222</sup> Technology opens avenues for children to express themselves, connect with others, and engage in the digital public sphere. However, these opportunities also expose them to potential risks, including misinformation and disinformation, which can undermine their rights and pose a threat to their well-being and development. The State has a responsibility to protect children from these dangers, ensuring that digital spaces support children's rights to association and freedom of thought while shielding them from misleading or harmful content.

Article 15 of the UNCRC affirms children's right to freedom of association and peaceful assembly. In the digital context, this right means that children must have access to platforms where they can connect with peers, share ideas, and engage in civic activities. Digital spaces can facilitate opportunities for association that transcend geographic and social boundaries, allowing children to participate in meaningful online communities. According to General Comment No. 25, the State has an obligation to ensure these online communities are safe, enabling children to exercise their right to association fully and securely.<sup>223</sup>

- 
- 217 Human Rights Watch, "'How Dare They Peep into My Private Life?' Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic' (2022) <<https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>> accessed 20 March 2025.
- 218 V Hillman, 'New study confirms that many EdTech companies exploit children's data and there is nothing to stop them', London School of Economic, (2022) <<https://blogs.lse.ac.uk/mediase/2022/05/25/new-study-confirms-that-edtech-companies-exploit-childrens-data-and-there-is-nothing-to-stop-them/>> accessed 20 March 2025.
- 219 A Atabey and L Hooper, 'International regulatory decisions concerning EdTech companies' data practices', 5Rights (2024), <[https://eprints.lse.ac.uk/123805/1/DFC\\_Brief\\_International\\_regulatory\\_decisions\\_final.pdf?\\_gl=1\\*1w6mu8v\\*\\_gcl\\_au\\*MTgwMTgxMzc3Ny4xNzI1MjkyMzcy\\*\\_ga\\*MTc5Nzc4MDQxOC4xNzI1MjkyMzcy\\*\\_ga\\_LWTEVFESYX\\*MTcyNTY1MjgwNC41LjEuMTcyNTY1MzIxNS42MC4wLjA](https://eprints.lse.ac.uk/123805/1/DFC_Brief_International_regulatory_decisions_final.pdf?_gl=1*1w6mu8v*_gcl_au*MTgwMTgxMzc3Ny4xNzI1MjkyMzcy*_ga*MTc5Nzc4MDQxOC4xNzI1MjkyMzcy*_ga_LWTEVFESYX*MTcyNTY1MjgwNC41LjEuMTcyNTY1MzIxNS42MC4wLjA)> accessed 20 March 2025.
- 220 Section 15 (f).
- 221 Australian Government, Australian E- Safety Commissioner, What we do, <<https://www.esafety.gov.au/educators/trusted-providers>> accessed 25 February 2021.
- 222 UN Convention on the Rights of the Child, Article 13; Article 14 and Article 17. 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 37 discusses the need to protect children's freedom of thought, particularly from manipulative digital content and algorithm-driven biases; para 78 and paragraph 79 emphasise the importance of providing children with access to reliable information and protecting them from misinformation and disinformation; para 82 addresses children's right to freedom of association in digital spaces and calls for secure, inclusive environments that respect this right.
- 223 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 82.

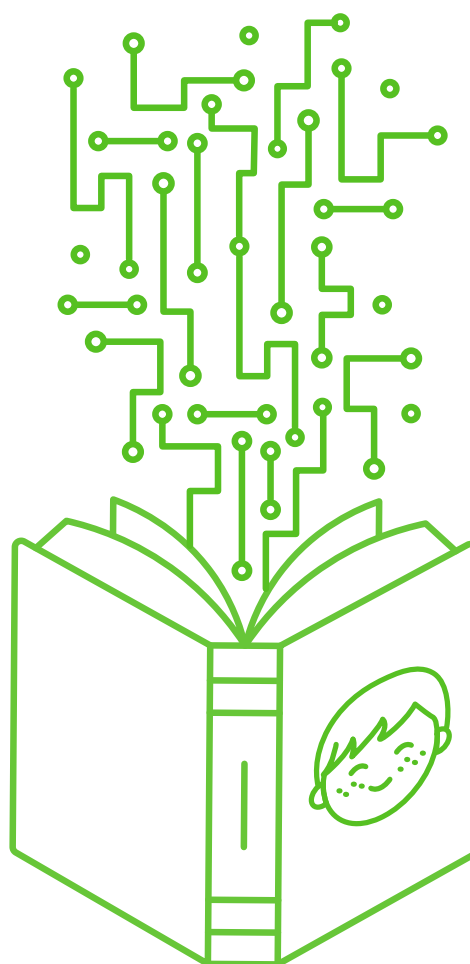
The right to freedom of thought, guaranteed under Article 14 of the UNCRC, is foundational to children’s personal and intellectual development. Digital platforms provide unique spaces for children to explore, question, and form their own beliefs and opinions. However, the digital environment can also pose threats to this right, particularly through business models that use algorithm-driven content, which may reinforce harmful biases or limit exposure to diverse perspectives, or may expose children and young people to violence.<sup>224</sup> To support children’s freedom of thought, the State must implement regulations that promote transparency in digital content algorithms and encourage platforms to provide a balanced range of information. These measures help safeguard children’s right to form and express their thoughts without undue influence from biased or manipulative digital content.<sup>225</sup>

The proliferation of misinformation (false or misleading information) and disinformation (information intended to deceive) in digital spaces poses a significant threat to children’s rights to access accurate information and form independent opinions.<sup>226</sup> As 5Rights Foundation has identified, some common design features of digital products and services create risks for young people which could be eliminated. These include poorly designed recommender systems.<sup>227</sup>

To ensure that products are not, as 5Rights Foundation puts it, ‘risky by design’,<sup>228</sup> the State, through regulation, must ensure that digital platforms take adequate steps to implement safeguards that avoid misinformation and disinformation, and provide children with reliable sources of information. These steps will include designing safe products in the first instance, and effective content monitoring to prevent misinformation and disinformation from reaching child users, as well as speedy and effective takedown of material that contains such harmful or illegal content. These safeguards should also include digital literacy programmes that educate children, educators, and others who care for

them or interact with them about recognising credible sources, verifying information, and critically engaging with online content. This protection aligns with Articles 13 and 17 of the UNCRC, which emphasise children’s rights to seek, receive, and impart information and ideas through media of their choice while ensuring their well-being.<sup>229</sup>

Online providers should create child rights friendly communities that protect children and young people’s right to association by allowing them to connect in monitored, age-appropriate spaces. This includes providing tools for children to interact safely, and report any threats to their safety and well-being, enabling them to exercise freedom of association without fear of harm or exploitation.<sup>230</sup>



224 *ibid* para 37, 38, 62.

225 *ibid* para 37.

226 United Nations Convention on the Rights of the Child (UNCRC) article 17 (Right to access to Information).

227 5Rights Foundation ‘Risky-By-Design – Brief on misinformation’ <<https://5rightsfoundation.com/resource/risky-by-design-brief-on-misinformation/>> accessed 27 November 2024.

228 *ibid*.

229 UN Convention on the Rights of the Child (UNGA Res 44/25, Arts 13, 17; UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children’s rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), paras 78, 79.

230 *ibid* para 82.

To protect freedom of thought, digital platforms should ensure children have access to a broad spectrum of information, sources, and viewpoints. Transparency in how content is curated or recommended to children is essential to prevent narrow information flows that can limit children's exposure to diverse perspectives and is required by the DSA.<sup>231</sup> This commitment supports children's right to explore ideas freely, contributing to a well-rounded intellectual and personal development.<sup>232</sup> It is for this reason that safety-by-design requiring recommender systems and algorithms based on personal data and user behaviour, disabled by default for child and young users is necessary to protect freedom of thought and access to information.

Digital literacy programmes along with product safety-by-design and privacy-by-design can empower children to become informed users, teaching them how to identify credible information sources, verify facts, and engage with content responsibly. These are essential to safeguard their right to access truthful information and fosters resilience against manipulative online content.<sup>233</sup>

## Awareness Raising

In addition to its obligations to keep children safe, the State also has a duty to proactively raise awareness about the unique risks children face online.<sup>234</sup> Such risks include threats such as child sexual abuse material (CSAM), grooming, cyberbullying, and exposure to harmful content - pornography, harmful or dangerous challenges, suicide ideation, self-harm, eating disorders, extreme violence, misogyny. According to Article 17 of the UNCRC, States must encourage the development of guidelines to protect children from information that may harm their well-being,

while General Comment No. 25 emphasises the importance of equipping children, caregivers, educators, and the general public with the knowledge to navigate the digital world safely.<sup>235</sup>

As such, the State must support and fund national public awareness campaigns designed to educate children and adults about recognising, reporting, and preventing online harms. These campaigns should empower children to make informed choices and educate adults on protective measures that promote children's rights to safety, information, and development.<sup>236</sup>

Effective online safety campaigns must adopt a comprehensive and strategic approach to protect children in the digital world. These campaigns should begin with early and age-appropriate education, ensuring children receive tailored information about the risks of generating or sharing sexual content.<sup>237</sup>

To maximise engagement, diverse and accessible formats, such as videos, posters, websites, and talks, games and quizzes should be used to reach children, parents, and the general public.<sup>238</sup> Active involvement of parents, caregivers and adults is essential, providing them with the knowledge to guide children and address risks effectively.<sup>239</sup> Collaboration between governments, educational institutions and NGOs can enhance outreach and effectiveness, leveraging shared expertise and resources.<sup>240</sup> Multi-channel strategies, including TV, online platforms, and public advertising, are critical for raising widespread awareness about child exploitation and online safety.<sup>241</sup> Incorporating proven good practices, like New Zealand's Keep it Real Online campaign effectively utilises a multi-platform approach to educate parents and children on online risks, demonstrating the power of government-led digital safety

231 The Digital Services Act (DSA) establishes transparency requirements for recommender systems in Recital 70 and Articles 27, 34, 35 and 38. Online platforms must clearly disclose how algorithms rank and present information, ensuring users understand the key criteria influencing content visibility, including profiling and online behaviour. Users should also have the ability to modify these parameters. For VLOPs and VLOSEs, additional obligations apply under Articles 33–43 relating to recommender systems.

232 Committee on the Rights of the Child, 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment', para 37.

233 *ibid* para 78.

234 *ibid* 32.

235 UN Convention on the Rights of the Child (UNGA Res 44/25, Art 17; UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 78.

236 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25, 2 March 2021), para 32.

237 Council of Europe, 'Promoting Awareness of the Risks of Sexual Exploitation and Abuse of Children' (Factsheet, 2022) 2, para 2.

238 *ibid*, 3, para 6.

239 *ibid*.

240 *ibid*, 3, para 7.

241 *ibid*, 3, para 8.

initiatives.<sup>242</sup> Similarly, Albania's #Openyoureyes and the Slovak Republic's Sheeplive project, can provide valuable inspiration for impactful initiatives.<sup>243</sup>

In Ireland, Coimisiún na Meán, as the State regulator, has undertaken the development of media resources on online safety. These have developed following consultation with its Youth Advisory Committee and others.<sup>244</sup> These resources are still at an early stage. There remains a pressing need for campaigns and awareness raising specifically addressing the online safety of children. In particular, a focus on child sexual abuse and exploitation, as well as other criminal offences targeting, exploiting, or causing harm to children online is needed; including raising awareness around the creation or possession of child sexual abuse material, the sending of sexually explicit material to a child, sexual grooming, and communications intended to facilitate the sexual exploitation of a child.<sup>245</sup>

In addition, online safety campaigns must comprehensively address all digital risks, encompassing harmful content, inappropriate contact, and unsafe conduct.

---

242 Department of Internal Affairs (New Zealand), *Keep It Real Online* <<https://www.keepitrealconline.govt.nz/>> accessed 14 March 2025.

243 Council of Europe, 'Promoting Awareness of the Risks of Sexual Exploitation and Abuse of Children' (Factsheet, 2022) 4, para 11.

244 Coimisiún na Meán, Information for students <<https://www.cnam.ie/information-for-students/>> accessed 20 March 2025.

245 Schedule 3 Broadcasting Act 2009 (Amended). 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).



## Education and Prevention Against Harm Online: Recommendations

- Establish a new cross- departmental Online Safety Action Plan to co-ordinate work ongoing across Government Departments.
- The Department of Education must review the Curriculum at both primary and post primary level in relation to Online Safety and embed online safety education that aligns fully with children’s rights in the digital environment across the curriculum.
- The Government must review and monitor EdTech applications for compliance with a child’s right to privacy and data protection standards and to safety, empowerment, learning and well-being across all learning environments.
- The Government must ensure that safety-by-design requiring recommender systems and algorithms that profile personal behaviour be disabled by default to protect the right to association, freedom of thought, and access to reliable information for children and young people.
- The Government must strengthen efforts to combat child sexual abuse material (CSAM) and increase understanding amongst the general public through targeted initiatives to raise awareness of online harms to children, focusing on child sexual abuse, CSAM, grooming, and sexual exploitation.

# Recommendations



# RECOMMENDATIONS

## Children's Rights in the Online World

- Amend Online Safety and Media Regulation (OSMR) Act to require the best interests of the child be the primary consideration in all aspects of online regulation and implementation, ensuring domestic alignment with these international obligations.
- Coimisiún na Meán's Youth Advisory Committee should be expanded without delay to include under-18s, ensuring direct child representation in online safety policy development.
- Online safety initiatives must include marginalised children, including Traveller and Roma children, children with disabilities, LGBTQI+ youth, and those from low-income backgrounds. Accessible, inclusive resources should be sustained and expanded, with tailored support for parents, caregivers, and educators to protect children online.

## Enforcing Regulation on the Online Industry

- Coimisiún na Meán should establish and operate an effective and accessible individual public complaints mechanism where end-user rights and protections are fully vindicated, and complaints made by children or involving a child are given priority. The Coimisiún must also:
  - Designate trusted flaggers to address children's online safety concerns;
  - Require platforms to prioritise complaints made by children, or involving a child;
  - Ensure the Appeals Centre Europe guarantee children timely and appropriate remedies;
  - Immediately act on all 'single serious infringements' where there is a potential risk of harm to a child.
- Coimisiún na Meán and the European Commission must strengthen oversight of platform compliance with the Digital Services Act. They must ensure accountability mechanisms are effective and child-centred. These must include safety-by-design, transparency, privacy and algorithms.
- The Government must lead reform of EU laws that combat the production, hosting, access and use of child sexual abuse material (CSAM). The Government must ensure these laws properly address grooming, encryption, detection and secure storage of both new and existing CSAM.
- Child Rights Impact Assessments could be made mandatory for platform policies to proactively mitigate risks against children and young people and to ensure a child-centred approach. CRAI must be fully integrated into the operations of Coimisiún na Meán.



## Education and Prevention Against Harm Online

- Establish a new cross- departmental Online Safety Action Plan to co-ordinate work ongoing across Government Departments.
- The Department of Education must review the Curriculum at both primary and post primary level in relation to Online Safety and embed online safety education that aligns fully with children’s rights in the digital environment across the curriculum.
- The Government must review and monitor EdTech applications for compliance with a child’s right to privacy and data protection standards and to safety, empowerment, learning and well-being across all learning environments.
- The Government must ensure that safety-by-design requiring recommender systems and algorithms that profile personal behaviour be disabled by default to protect the right to association, freedom of thought, and access to reliable information for children and young people.
- The Government must strengthen efforts to combat child sexual abuse material (CSAM) and increase understanding amongst the general public through targeted initiatives to raise awareness of online harms to children, focusing on child sexual abuse, CSAM, grooming, and sexual exploitation.





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.

7 Red Cow Lane Smithfield,  
Dublin 7,  
D07 XN29 Ireland  
Ph: +353 1 662 9400  
Helpline: +351 1 902 0494  
Email: [info@childrensrights.ie](mailto:info@childrensrights.ie)

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

Companies Registration Number: 316758  
Charity Number: CHY 11541  
Charity Registration Number: 20031909

© 2025 Children's Rights Alliance  
Republic of Ireland Limited