Submission from

Athlone Midland Rape Crisis Centre
Dublin Rape Crisis Centre
Galway Rape Crisis Centre
KASA Kilkenny
Sexual Violence Cork
Sligo Rape Crisis Centre
Tullamore Rape Crisis Centre
Wexford Rape Crisis

on developing Ireland’s first binding online safety code for video-sharing platform services

September 2023

▶ Rape Crisis Centres

Rape Crisis Centres (RCCs) provide crisis counselling and long-term therapy to those who have experienced rape, sexual assault and childhood sexual abuse. The services include helplines and associated services, one-to-one counselling, medical, Garda and court accompaniment, education and training programmes, policy interventions, public awareness campaigns to prevent sexual violence and data collection and analysis on trends and issue relating to sexual violence. The work carried out by RCCs has prompted social, political and cultural changes in Ireland.

The following RCCs work together on common issues as members of the Rape Crisis Centre Managers Forum and constitute half of all the Rape Crisis Centres in Ireland.

We are:

1. Athlone Midland Rape Crisis Centre;
2. Dublin Rape Crisis Centre;
3. Galway Rape Crisis Centre;
4. KASA Kilkenny;
5. Sexual Violence Cork;
6. Sligo Rape Crisis Centre;
7. Tipperary Rape Crisis Centre;
8. Tullamore Rape Crisis Centre; and
9. Wexford Rape Crisis.

As frontline service providers, we work with and support people who have been directly affected by sexual violence including online abuse. Through that work, we see the often life-long consequences of the trauma and harm caused by sexual violence of all kinds. We also know from our experience that often this harm is because of digital technology that is used to harass and humiliate.

Eight of our colleague organisations from the Forum; Athlone, Dublin, Galway, Kilkenny, Cork, Sligo, Tullamore and Wexford join with us in making this submission which is informed by the experiences of the women and men accessing these services who are victims of sexual violence.

▶ About this submission

We welcome the opportunity to contribute to this consultation process. We have structured our responses in the form of answers to the questions set out in the consultation document. In addition, we support the submission being made by the Children's Rights Alliance on behalf of a coalition of organisations including Dublin Rape Crisis Centre. The particular focus of that submission relates to children and young people but is equally applicable to the wider population, in particular those who are additionally vulnerable because of age, gender, relational abuse or other issues.

- **Questions and responses**

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

Ireland's first binding Online Safety Code (the Code) should be the benchmark for requiring VSPS providers to protect online users from harm by ensuring their services make appropriate use of systems and process to keep users safe. Some of the main priorities and objectives that should be considered are:

- User Safety and Well-being:
  - The primary objective should be to safeguard users from various forms of online harm and ensure their safety, well-being and privacy.

- Platform Responsiveness:
  - Put time limits in place for providers to remove illegal or harmful content upon identification. Require platforms to impose proportionate sanctions on perpetrators including account suspension and termination.

- Transparency and Accountability:
  - Users should know how decisions about content removal are made. The providers should publish regular reports that include content moderation and enforcement actions.

- User Empowerment:
  - Promote collaboration between the providers and educational institutions to promote digital literacy. Require providers to promote awareness among users of the avenues of complaint and redress available to them.

- Regular Review and Update:
  - Ensure regular reviews and updates to adapt to new challenges in the ever-evolving online environments.

The Code should address a wide range of online harms to create a safer and more secure digital environment. Many of these harms can have a significant negative impact on individuals, communities, and society as a whole. Included in the harms the Code seeks to address should be those outlined in Article 28b of the Audiovisual Media Services Regulation[1] and all the categories of harm set out in the Broadcasting Act 2009 as amended by the Online Safety & Media Regulation Act 2022.[2]

In particular, the Code should address technology-facilitated gender-based violence (TFGBV). Technology-facilitated GBV refers to any act that is committed, assisted, aggravated or amplified using Information and Communication Technologies (ICTs) or

[1] EU's Audiovisual Media Services Directive: https://eur-lex.europa.eu/eli/dir/2018/1808/oj

[2] Online Safety & Media Regulation 2022: https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/print.html

other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms.[3]

In our work, we regularly hear from those using our services that the abuser, who may be known to them or not, posts or threatens to post intimate images of them without their consent to humiliate, intimidate, or blackmail them. Survivors of sexual violence can be subjected to online trolling or negative and abusive commentary which can be incredibly harmful to them personally and can also have a broader effect of deterring victims/survivors from seeking help or reporting their assault. Recently, DRCC launched an anonymous online platform where survivors of sexual violence can share their stories without fear of being trolled. The purpose of We-Speak[4] is to provide a platform for survivors of sexual violence to reclaim their narrative and safely tell their own stories.

The Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW) first thematic paper on the digital dimension of online abuse describes online and technology-facilitated violence against women as having a devastating impact on women and girls, and society generally. It is often experienced as an all-encompassing harm impacting on every aspect of their lives, leading to a form of 'social rupture' where lives are divided into 'before' and 'after' the violence.[5] These are sentiments echoed by those using RCCs in terms of the devastating impact the online harm had on their lives and why it is so important that they are addressed.

The Code should proceed on the understanding that violence or harm perpetrated online is just as serious as harm perpetrated offline. Perpetrators of technology-facilitated GBV should not be enabled to evade accountability or hide behind a veil of anonymity by reason of weak or inadequate procedures imposed by VSPS providers. Users subjected to technology-facilitated GBV suffer real life impacts and harms and must have clear access to remedies and supports.

The UN Human Rights Council has long-since clarified the principle that human rights protected offline should also be protected online.[6] Indeed, the UN special Rapporteur on Violence against Women, Its Causes and Consequences warned, in 2018, of the significant risk that the use of ICT without a human rights-based approach and in the absence of the prohibition of online gender-based violence could broaden sexual and gender-based discrimination and violence against women and girls in society even further.[7]

[3] See Technology-facilitated Violence against Women: Towards a common definition Report of the meeting of the Expert Group 15-16 November 2022, New York, USA available at https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf
As acknowledged in the expert group report, technology-facilitated violence disproportionately impacts women in all their diversity and gender non-conforming individuals; it is noted that "violence against women" (VAW) can be substituted with "gender-based violence" (GBV), whilst maintaining the common definition describing the phenomenon.

[4] https://www.wespeak.ie/

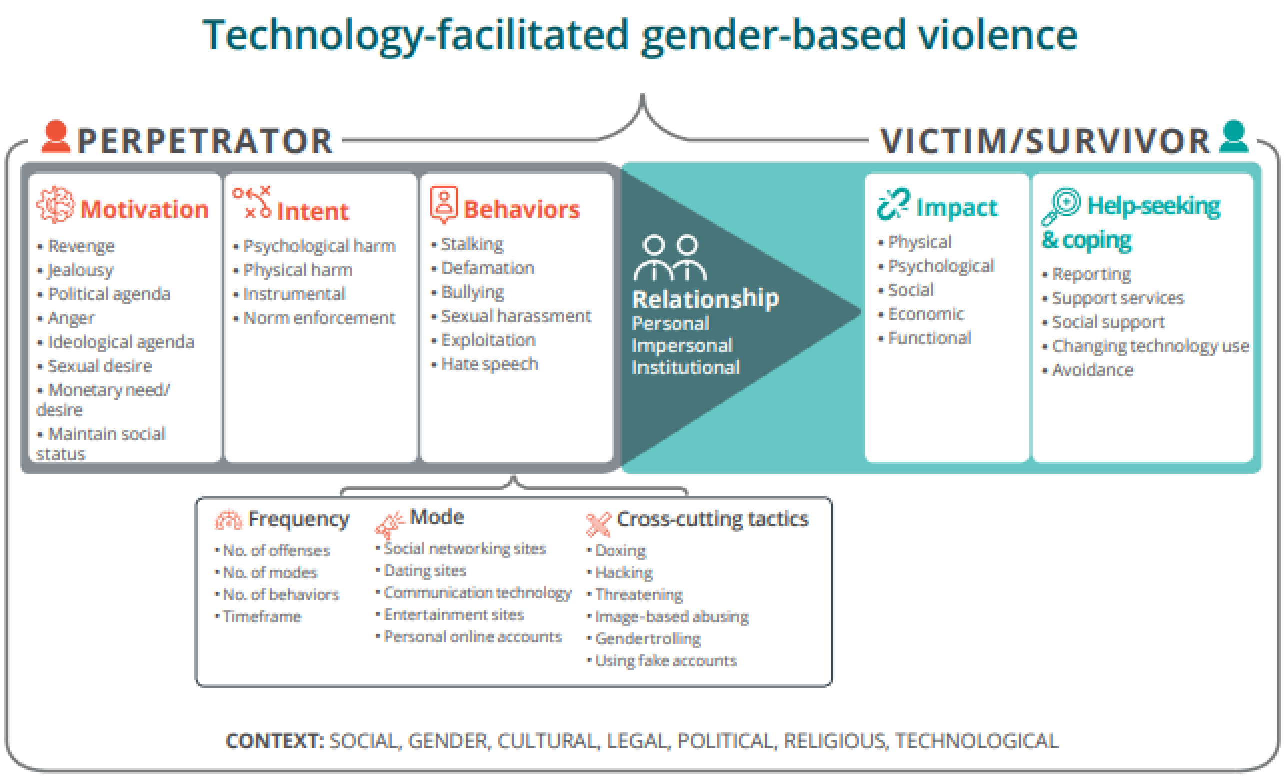
[5] Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform)): *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform* (2021), available at: https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_English.pdf

[6] Human Rights Council resolution 32/13.

[7] Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective at para 19 available at https://digitallibrary.un.org/record/1641160?ln=en

A primary objective of the Code should be to combat and prevent the ever-evolving forms of technology-facilitated GBV, while upholding the right to freedom of expression, including access to information, the right to privacy and data protection, as well as the rights of women that are protected under the international human rights framework.

For the purposes of the Commission's research and preparation of the draft Code, we refer to the research published by the International Centre for Research on Women who produced the following infographic to help summarise the conceptual framework in which technology-facilitated GBV sits:[8]



© 2018 International Center for Research on Women (ICRW). All rights reserved.

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

Using technology and being online is an integral part of everyone's life, including for education, employment and social interactions. However, if the devices we use become sites of trauma as a result of online abuse, then the knock-on effect of that abuse is one that directly and adversely impacts every aspect of our lives.

[8] Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018). Technology-facilitated gender-based violence: What is it, and how do we measure it? Washington D.C., International Center for Research on Women available at https://www.icrw.org/wp-content/uploads/2018/07/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

Covid-19 exacerbated online and technology-facilitated GBV[9] and a number of studies suggest that the current prevalence of digital violence is high, mostly impacting young women and girls, women in public life, and people with intersecting identities. [10] [11] According to the EU Agency for Fundamental Rights' survey on violence against women (2014), 14% of women in the EU have experienced stalking in the form of offensive or threatening communications since the age of 15.[12] A report commissioned by Women's Aid shows that 1 in 5 young women and 1 in 11 young men in Ireland have suffered intimate relationship abuse. In all cases where women were subjected to intimate relationship abuse, this abuse was perpetrated by a current or former intimate male partner.[13] According to the report *Toxic Twitter* issued by Amnesty International, 25% of respondents polled across eight countries had received threats, including of sexual violence, physical pain, incitement to suicide and death towards them and their family on Twitter. [14] Plan International, found that more than half of the interviewed 14 000 15 to 25 year old women from 22 different countries said they had been cyberstalked, sent explicit messages and images, or abused online.[15]

The harms of key concern to RCC's where the most stringent measures need to be applied relate to:

- Intimate image abuse (IIA)[16]
- Technology-facilitated GBV the range and extent of harms which arise online, and which disproportionately impact women, girls and LGBTI individuals.[17]
- Cyberbullying and online harassment
- Child Sexual Abuse Material (CSAM), Child Sexual Abuse Imagery (CSAI), child pornography
- Child Sexual Exploitation (CSE) and technology facilitated child sexual exploitation
- Computer generated or drawn content depicting gross child sexual abuse[18]
- Non-consensual posting of a person's details on escort websites/OnlyFans etc (whether intimate image abuse involved or not)

[9] The Ripple Effect: COVID-19 and the Epidemic of Online Abuse by Glitch UK and End Violence Against Women Coalition available at https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf.

[10] See Practice Brief on Innovation and Prevention of Violence Against Women issued by UN Women, July 2023 available at https://www.unwomen.org/en/digital-library/publications/2023/07/innovation-and-prevention-of-violence-against-women

[11] The Ripple Effect: COVID-19 and the Epidemic of Online Abuse by Glitch UK and End Violence Against Women Coalition (above). This survey found that "gender was the most often cited reason for online abuse. 48% of respondents reported suffering from gender-based abuse; 21% of respondents reported suffering from abuse related to their gender identity and sexual orientation, followed by 18% for their ethnic background and 10% for their religion and 7% for a disability."

[12] Fundamental Rights Agency (2014), '*Violence against women: an EU-wide survey. Main results report*', available at https://fra.europa.eu/en/publication/2014/violence-againstwomen-eu-wide-survey-main-results-report

[13] Women's Aid (2020), 'One in Five Young Women Suffer Intimate Relationship Abuse in Ireland', available at https://www.womensaid.ie/app/uploads/2021/03/one_in_five_women_report_womens_aid_2020.pdf

[14] Amnesty International (2018), '*Toxic Twitter, a toxic place for women*', available at www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1

[15] Plan International (2020), '*Free to be online? A report on girls' and young women's experiences of online harassment*', available at https://plan-international.org/publications/freetobeonline

[16] Intimate image abuse has previously been referred to as 'revenge porn' which is widely accepted now as wholly inappropriate.

[17] See Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018). Technology-facilitated gender-based violence: What is it, and how do we measure it? Washington D.C., International Center for Research on Women available at https://www.icrw.org/wp-content/uploads/2018/07/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

[18] 9% of CSAM assessed by Hotline.ie in 2021 was computer generated. It would often then contain a disclaimer that '*no child has been harmed in the process*'. Hotline.ie 2021 Annual Report, p.15: https://hotline.ie/library/annual-reports/2022/Hotline.ie-AR21-webready.pdf

- Doxing - posting a person's private details online such as their address or phone number without their permission and with the aim to cause alarm or distress
- Victims of trafficking being displayed on escort websites
- AI/Computer generated or drawn content depicting a person's identity without consent, especially where it constitutes an intimate image or contains sexual violence.

In 2021, Hotline.ie the national reporting centre for illegal online content received the highest number of reports in one year, 29,794 reports compared with 10,699 the previous year. The images involve a victim(s) who have suffered abuse but who go on to be re-victimised each and every time the image of their abuse is viewed. The 2021 report also included, for the first time, statistics on intimate image abuse (IIA), or the non-consensual sharing of intimate images and videos. Between September 2021 and September 2022, Hotline.ie received 773 reports of suspected IIA. Hotline report that 83% of victims of IIA processed by Hotline.ie are female; 16% male and 1% prefer not to say. DRCC helpline staff have noted an increase in male victims reaching out for assistance and support in recent months.

Evidence also suggests that there is a clear, but often overlooked, overlap between online and offline (or in person / physical) abuse and violence. Perpetrators may target a victim in multiple ways simultaneously. For example, a perpetrator of in person intimate partner abuse may, either during the relationship or at the point their partner ends the relationship, turn to online forms of harassment, abuse and extortion.[19]

Platforms and their moderators require specialised training in identifying and understanding domestic, sexual and gender-based violence (DSGBV) and to understand the dynamics of consent, control, coercion and harm. In a survey carried out in the UK regarding online abuse during the Covid-19 pandemic, 83% of respondents who reported one or several incidents of online abuse during COVID-19 felt their complaint(s) had not been properly addressed. This proportion increased to 94% for Black and minoritised women and non-binary people.[20]

The Code must ensure that illegal material such as child sexual abuse materials and intimate images are removed quickly.

Providers should provide more transparency about their policies related to online abuse, including their position as regards dehumanising language based on gender, ethnicity and other protected categories. Providers should engage actively and regularly with experts in the field of GBV (and child protection) and regularly review and update policies to address new trends, patterns and manifestations of online abuse, including violence against women and people with intersecting identities.

[19] See Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018). Technology-facilitated gender-based violence: What is it, and how do we measure it? Washington D.C., International Center for Research on Women at https://www.icrw.org/wp-content/uploads/2018/07/ICRW_TFGBVMarketing_Brief_v8-Web.pdf
See also UN Women Brief: The state of evidence and data collection on technology-facilitated violence against women, 2023 available at https://www.unwomen.org/en/digital-library/publications/2023/04/brief-the-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women which cites Messing et al.'s interviews with residents of a women's shelter which helped illustrate how technologies are interwoven throughout women's experiences of stalking and abuse, making the distinction between 'offline' and 'online' violence blurry – especially given women's need to continue using digital technologies for their livelihoods and, indeed, to escape situations of violence.

[20] The Ripple Effect: COVID-19 and the Epidemic of Online Abuse by Glitch UK and End Violence Against Women Coalition (above).

Some early-stage research is currently investigating the dichotomy between what types of harmful content online platforms seek to curb and what research efforts there are to automatically detect such content. The research paper discusses the mismatch in focus as well as other challenges to be addressed in addressing online harms including fluid policies and platform responsibility and directions for future work.[21]

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

We would support option 1 in the consultation paper that the Code should be a very detailed prescriptive Code that could specify in detail the measures the VSPS would be expected to take to address online harms.

Non-binding guidance should not be utilised in a way which would dilute or obfuscate the obligations on providers to remove harmful content within specified, rapid timeframes, to have proportionate and effective age-identification mechanisms in operation, to offer users clear and accessible channels to report harmful content and to take proportionate steps against perpetrators of harm (including suspension and termination).

We believe the Code should address content connected to video content including comments on videos, descriptions of videos or text and images embedded with videos. We would additionally suggest that this extends to links cited in or under video content which leads to harmful content elsewhere on the internet (an obvious example here would be a link to an adult pornography website embedded in content available to children).[22]

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

We support age verification. There must be a level of thoroughness proportionate to the risk of harm due to the nature of the content on the platform. For online users whose age cannot be verified or assured, the default content should prioritise safety and appropriateness and show content that is suitable for all audiences.

[21] *Detecting Harmful Content on Online Platforms: What Platforms Need vs. Where Research Efforts Go* was accepted to ACM Computing Surveys https://dl.acm.org/doi/epdf/10.1145/3603399

[22] *Children exposed to 'vast amounts' of inappropriate content online* (September 2022) https://www.rte.ie/news/2022/0906/1320777-cyber-safety-ireland/

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

VSPS providers should see media literacy measures and tools as a foundational necessity in being involved in the digital world. It is not enough to have good terms and conditions and safety features in place, if the users of the technology are not enabled to actively engage with them. VSPS providers must roll out accessible, age-appropriate educational initiatives to help users understand how to stay safe online, how to respond to online abuse and how to be an active online bystander. Providers should engage the expertise of organisations working in the field of child protection and GBV.

Question 14: How should we ask VSPS providers to address online harms in their terms and conditions in the Code, including the harms addressed under Article 28b? How should key aspects of terms and conditions be brought to users' attention? What examples are there of best practice in relation to terms and conditions including content moderation policies and guidelines?

Transparency and simplicity are key in bringing the terms and conditions to users' attention. The key terms in plain user-friendly language, without the use of jargon or legalese should be prominently displayed during the registration or sign-up process to ensure users see them before proceeding. The use of visual cues like graphics or symbols to draw attention to important aspects or interactive features that require user engagement could be included to ensure the key aspects of the terms and conditions are brought to users' attention.

Strict implementation of a provider's terms and conditions is vital. Rapid Take Down Protocols, together with account suspensions and terminations, will send an unambiguous message to perpetrators and potential perpetrators that such abuse will not be tolerated, which in itself can have a preventative impact.

The Code should also require providers to actively establish and utilise systems to identify repeat offenders of online abuse. Anonymity is a key tool utilized by persons intent on causing harm online. Providers should be required to take steps to make it far more difficult for accounts that have been the subject of a ban or termination to resurface as a new account.

Question 16: What requirements should the Code include about procedures for complaint-handling and resolution, including out-of-court redress or alternative-dispute resolution processes? To what extent should these requirements align with similar requirements in the DSA? What current practices could be regarded as best practice? How frequently should VSPS providers be obliged to report to the Commission on their complaint handling systems and what should those reports contain? Should there be a maximum time-period for VSPS providers to handle user complaints and if so, what should that period be?

Time is of the essence for intimate image abuse (IIA), the longer it takes to remove content, the greater the risk of repeat victimisation. Once an intimate image is online, it is very easy to copy, save, replicate and spread. Action needs to be immediate. The user should be enabled to make their complaint directly to the VSPS provider, who should proceed based on accepting the truth of a statement of non-consent and should promptly remove the content. **A precautionary approach in favour of removal is appropriate here.**

Whether consent was forthcoming or not at the time the image was uploaded is irrelevant to the question of removal as consent can be revoked. The key facts relevant to the platforms should be whether the image in question is of the complainant. The facts and evidence around consent (if non-consent is contested by the user who posted the image/video) are primarily relevant to any criminal investigation An Garda Siochána undertake, and platforms should preserve all relevant evidence for same. Such questions may also be relevant to any decision the provider takes as regards a sanction against the user who posted/hosted the disputed image or in respect of any review that user may take against a decision to take down or to suspend/terminate their account. However, as time is so vitally of the essence in the case of IIA, removal on a precautionary (and possibly temporary) basis should be the default with providers conducting any more detailed factual investigations only thereafter.

If the offending content is not taken down or a notice not complied with in a take-down timeline specified in the Code, then the user should have access to an accessible and effective complaint mechanism. The complaint mechanism should offer a very prompt internal review of the initial decision so that legitimate requests to takedown harmful content are not unduly delayed which would in turn result in serious and escalating harm to the user/victim. The user should also be offered an avenue to seek an external review of a complaint to an independent body such as the Commission.

In the case of harmful content of a sexual or intimate nature such as IIA[23] and CSAM, the time-frames in question for both an initial moderation decision on a take-down request and a complaint/request for a review should be in the order of hours not days i.e. an initial decision should be taken within 12-24 hours and a review decision should be the same in cases whether the disputed content remains online. Once, and for so long as, the disputed content is removed (even temporarily), longer timeframes may be acceptable for the processing of final decisions and reviews/complaints.

The Code should not require any person to engage in mediation with a perpetrator of harm or GBV. Out of court redress or alternative dispute resolution processes such as mediation may be relevant and appropriate to a dispute between users and VSPS providers but only in cases where the user consents to such processes. Education and awareness raising of user's rights in this respect should be rolled-out.

VSPS providers should submit quarterly reports on the measures and actions they have put in place to combat harmful and inappropriate content. These reports should contain comprehensive data and details as regards users experience of the VSPS provider's platform and complaint handling systems. This data should include details of the number of take-down requests received, the number acted on and the number dismissed, the number of account suspensions and terminations, the number of user complaints received and the outcome of same. All data should be anonymised and disaggregated by age and gender of perpetrator(s) and victim(s) where known and the nature of the disputed content. In this ever evolving and growing digital space, such data and detail is necessary

[23] Content which includes a person's image and contact details or a suggestion that the person is seeking or available for intimate contact where that person has not consented should also be treated with the utmost urgency in moderation and take-down decisions.

to enable the Commission, researchers and users to understand what is working, what is not working and what changes and updates are necessary.

VSPS providers should also be required to report on their digital literacy efforts and training initiatives, to include details of the nature of specialised training moderators and staff involved in design and safety features receive in relation to child protection and GBV matters. Ultimately the reporting and resolution mechanisms must be effective, transparent, easy to access and easy to use.

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

Ensuring that the safety measures required by the Code are accessible to people with disabilities is essential to creating an inclusive online environment. VSPS providers should be required to adhere to recognised accessibility standards such as the Web Content Accessibility Guidelines (WCAG) 2.1,[24] alt text for images, keyboard navigation, and screen reader compatibility to ensure that their safety measures are accessible. Terms and conditions and reporting procedures should be available in alternative formats i.e., audio, braille, or plain text for users with various disabilities.

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

Security-by-design, privacy-by-design and user safety considerations should be standard requirements in product/service development by VSPS. Impact/risk assessment frameworks should be applied with appropriate checks and balances.

Question 20: What approach do you think we should take in the Code to address feeds which cause harm because of the aggregate impact of the content they provide access to? Are there current practices which you consider to be best practice in this regard?

It is vital for providers (and their design staff and moderators) to have an evidentially informed understanding of GBV to be able to design safety features and assess user complaints effectively. For example, most of the literature tends to discuss incidents of abuse as single events requiring a moderator to consider a single video/comment/post and to make a decision on that individual item. However, this ignores the multiple acts of abuse and violence a person may experience online, potentially across platforms, and simultaneously offline. A perpetrator of abuse may engage in stalking, defamation, bullying, sexual harassment, exploitation and/or hate speech. These may be repeated behaviours carried out across multiple platforms. Alongside speedy moderation processes for single events which obviously constitute abuse or illegal behaviour, there should also be channels for users to report accounts carrying out multiple behaviours which culminate in abuse against a user (or group of users) even where each single incident in isolation may not establish the abuse.

[24] Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/

Question 22: What compliance monitoring and reporting arrangements should we include in the Code?

To be effective, all VSPS providers need to be subject to the Online Safety Code – any platform that seeks to evade the obligations under the Code undermines the objective of making online activity safer for children and all users. Those intent on perpetrating harm will favour the platforms that seek to remain outside the Code or other Regulations (perpetrators are known to employ '*platform hopping tactics*'[25]). RCCs are concerned that the effective progression and implementation of these and similar measures may be greatly undermined should platforms bring about delays through avoidable court proceedings on technical points or matters that could be pre-empted and avoided at this early juncture.[26] This consultation is key to seeking to address all concerns and viewpoints of all relevant actors in the hope of avoiding such delays. Equally, RCCs assumes platforms will adopt a reasonable and proactive approach to assisting the Commission adopt an online safety code that is effective, practicable and acceptable to all.

For further information, on behalf of the group, please contact:

shirley.scott@rcc.ie	**| 01-6614911 ext. 124**
aoife.gillespie@rcc.ie	**| 01-6614911 ext. 116**

National 24-Hour Helpline: 1800 77 88 88

[25] See Hotline.ie Annual Report 2021 p.16. Hotline.ie also note perpetrators use '*breadcrumbing*' tactics to essentially leave an innocuous trail of clues across various websites to eventually lead to CSAM i.e. as a form of distribution.

[26] See EU safety laws start to bite for TikTok, Instagram and others, BBC News 25 August 2023 (here) which details: "*Retailers Zalando and Amazon have mounted legal action to contest their designation as a very large online platform. Amazon argues they are not the largest retailer in any of the EU countries where they operate. Nevertheless, Amazon has taken steps to comply with the act and has "created a new channel for submitting notices against suspected illegal products and content". Zalando told the BBC it will be compliant with the act.*"