

# Your response

## Volume 2: The causes and impacts of online harm

### Ofcom's Register of Risks

#### Question 1:

i) Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

1. Volume 2 is a commendable document within the suite of Ofcom's consultation materials. There has been clear and rigorous work to assess and register the causes and impacts of online harms.
2. CCDH believes that Volume 2 is the strongest standalone document contained within the consultation. That assessment forms the basis of our advice in this section and by way of comparison to the following volumes.
3. CCDH is concerned that the detailed evidence populating Volume 2, though itself commendable, is insufficiently translated into the draft Codes of Conduct in Volume 4.
4. For all the work Ofcom has put into assessing the causes and impacts of online harms in Volume 2, the assessment does not flow through to the mitigation measures it sets out later. In Annex 7, for user to user services, and Annex 8, for search services, the focus is primarily on content takedown and measures to deal ex-post with illegal content once identified.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

5. **Analysing the risk and illegality of steroids and steroid-like drugs** - Volume 2 6H summarises the risks of harm from the supply, or offer to supply, of drugs and psychoactive substances. CCDH research has evidenced the widespread promotion of steroid and steroid-like drugs on user to user services.
6. These drugs are illegal for human consumption. The flourishing trade in these products is owed to a grey area in which the drugs can be sold for research purposes legally, but are clearly marketed towards human consumption - which *is* illegal.
7. CCDH's report "[TikTok's Toxic Trade](#)" (2023) found TikTok influencers promoting steroid-like drugs that are illegal to sell in the UK and dangerous for human consumption, in some cases directing users to sites selling them with discount codes and affiliate links. Such content exacerbates the vulnerabilities of users by promoting unrealistic and unhealthy body image ideas, potentially leading to dangerous health outcomes.
8. Researchers examined hashtags relating to three classes of steroids and steroid-like drugs: anabolic-androgenic steroids, peptides, and Selective Androgen Receptor Modulators. Using TikTok's own tools to analyse the viewership of videos featuring 26 popular hashtags, CCDH revealed that content promoting dangerous steroid-like drugs had been viewed 117 million times by UK users.
9. Researchers also discovered that influencers posted paid content promoting the sale of steroid-like drugs to their followers, many with affiliate marketing schemes involving 13 separate vendors.
10. From this research, it is clear that video sharing platforms have insufficient systems in place to enforce their own rules prohibiting the sale and promotion of illegal substances.

Selling these substances in the UK is a criminal and there is extensive evidence showing the consequences they have for the body. The consequences are even more extreme when consumed by minors who have not finished body maturation (puberty).

11. User base risk factors are in play here, as video sharing platforms like TikTok are predominantly used by young users, for whom these drugs can have the most extreme consequences.
12. In light of this evidence and to place a premium on action for platforms like TikTok which have served a central role in facilitating the trade in illegal steroids and steroid-like substances, CCDH suggests explicit mention be made in Volume 2 (and later in Volume 5) about this area of drug offences.
- 13. Registering the role of third-party services operating on regulated platforms in the illegal drug trade** - in the same report, "TikTok's Toxic Trade", CCDH detailed the role of third-party linking services, known as "link in bio" tools such as Linktree or Direct.me.
14. Volume 2 8.97 is explicit in the requirement for services to "require due diligence of third-party contractors or providers of services involved" in the supply chain, but what about third-party services on the other end of the user journey?
15. CCDH believes that references to third-party involvement here in Volume 2, and later in Volume 3, should be increased given the extensive evidence about the role of third-parties in linking to or facilitating the journey from a regulated service to a digital marketplace or supplier. These very limited references to the risks of supply chain/third party involvement are despite Volume 2's recognition that many services are relying on third-party software and services like link-in-bio providers.
16. Finally, CCDH would note that the analysis on the functionalities related to user access to illegal content via search services is presented differently in Volume 2 than from elsewhere in the consultation documents: a high-level summary narrative that talks about functionality in relation to particular offences, rather than an offence-by-offence analysis. CCDH is partial towards greater inclusion of this narrative form, high-level and summarising desired outcomes, in future versions of these codes and guidelines.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

## Volume 3: How should services assess the risk of online harms?

### Governance and accountability

#### Question 3:

i) Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?

1. CCDH agrees that governance and accountability processes are vital for a service to identify and address online safety risks.
2. CCDH particularly commends the introduction, at 9.8, where Ofcom makes clear “Our goal is that services prioritise assessing the risk of harm to users (especially children) and run their operations with user safety in mind. This means putting in place the insight, processes, governance and culture to put online safety at the heart of product and engineering decisions.”
3. However, Volume 3 appears to contain an underlying assumption that governance and accountability processes are in one of two states: (1) *not* in place, and thus needing to be started from scratch, or (2) already in operation and sufficient. On the latter, CCDH would point out that there are indeed many governance and accountability processes operating, but that these processes are primarily about managing corporate risk, rather than the risk to users from illegal content.
4. Meta [whistleblowers](#) like Francis Haugen and Arturo Bejar have exposed highly sophisticated governance and assessment processes operating within the social media company. Their evidence shows senior managers are [often aware](#) of user safety risks, including those from illegal content. The failure of these processes to address harms in-scope of the OSA suggests much more rigorous governance and accountability measures are necessary.
5. The governance and risk assessment proposals seem to take at face value communications from regulated services that claim to be doing much of this already (pg 6, 11, 13, etc). CCDH does not accept this at face value.
6. CCDH also questions where non-priority offences are considered in the governance approach. For example, in emerging harms the consultation proposes tracking evidence of new kinds of illegal content, saying that “U2U services should track and report equivalent changes in the use of the service for the commission or facilitation of *priority offences*”.

ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

7. CCDH is concerned with weakness in the sections following 8.108, “Tracking evidence of new and increasing illegal harm”.
8. Particularly in 8.117, Ofcom highlights current practices by large user to user and search services including Meta, Google, and YouTube. It is reasonable to reference these practices, but CCDH is concerned that benchmarking those processes gives the impression that they are sufficient to meet the aims of the internal assurance and compliance functions required by the OSA.

9. The processes noted in 8.117 are essentially user risk identification processes used for the identification of *corporate* risk and business threats. While these have relevance to illegal harms and were pointed to by these platforms in their response to Ofcom’s 2022 Illegal Harms Call for Evidence, they are not processes designed for the primary purpose of user safety.
10. Indeed, CCDH has compiled extensive evidence of the practices commended in 8.117 as insufficient to secure user safety in the face of emerging trends and technologies. In our report “[Horizon Worlds Exposed](#)” (2023), CCDH documented extensive failures by Meta to institute basic user safety in its Metaverse products. Even following CCDH reporting on risks to minors when the app was purportedly 18+, Meta pushed forward with plans [to officially open](#) the VR product to minors.
11. In CCDH’s report “[AI and Eating Disorders](#)” (2023), our researchers showed how these emerging technology products, including Google’s Bard AI, generated harmful eating disorder content in up to 41% of tested results.
12. Ofcom should be cautious about representations from industry, particularly if those are representation of good practice and reassurance that industry is doing all it can. CCDH believes it is a misstep for 8.117 to highlight current measures large services take to assess emerging illegal content risks when it is those same services that launch markedly unsafe new technology products.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

#### Question 5:

i) Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?

1. The nascency of online safety regulation means there is only limited evidence concerning independent third-parties auditing digital platforms for illegal content risk management.
2. At present, there are a limited number of entities capable of conducting large-scale audits of the largest platforms regulated under the OSA. Some of those theoretically capable are [irreparably compromised by existing ties to industry](#) and a litany of auditing failures related to profit prioritisation.
3. CCDH believes that the [large-scale failure](#) of [major auditing firms](#) must be kept in mind when designing future requirements for the audit of regulated services. Ofcom should therefore foster optimal conditions for a diversity of audit practitioners with high levels of independence from commercial interests.
4. Fundamentally, CCDH believes this is further evidence of the need to **increase data access for academics and non-academic experts in civil society**. Breaking the current status quo of information asymmetry, which has allowed platforms to (1) deny the extent of the illegal content risks on their platforms or (2) hide behind rubber stamp “audits” from compromised auditors, is critical to fostering an efficacious auditing environment.
5. Fostering optimal conditions will require a diversity of auditors and auditing organisations with high levels of independent data access and research competency. This cannot be

achieved by relying on compromised auditing firms and without widening data access to independent researchers.

6. CCDH has evidenced [the rapid erosion of transparency](#) and data access pathways which had previously been used to independently [assess platforms' successes and failures](#) in mitigating illegal content risks. To give just one example, CCDH used the TikTok Creative Center to assess the viewership of different types of content on the platform, including [suicide and eating disorder promotion](#) and disinformation related to the October 7th terrorist attack in Israel. In 2023, viewership data was provided for hashtags when searched in the TikTok Creative Center. However, apparently in response to criticism,, [TikTok no longer displays](#) how many times videos with a specific hashtag have been viewed.
7. This is just one example of the restrictive efforts many platforms regulated under the Online Safety Act have taken against independent and effective oversight. For this reason, CCDH urges Ofcom to work to increase transparency and **data access pathways for researchers** as a **necessary component of efficacious auditing** under the illegal harm duties, but also in future stages of the online safety regime dealing with children and user empowerment.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

#### Question 6:

i) Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?

1. CCDH is aware of the societal impacts caused by senior managers at technology companies who receive enormous compensation without repercussions for the consequences of their products.
2. Ofcom is right to identify the misalignment of business incentives and online safety. Introducing a layer of accountability to the regulator via the threat of personal financial penalty can counterbalance the destructive privileging of shareholder value over online safety outcomes.
3. At present, the factors contributing to senior manager remuneration are opaque. This lack of transparency obscures key incentives driving senior manager behaviour and business choices. CCDH supports Ofcom scrutinising these incentives, particularly at board-level and for shareholder accountability. Realigning these perverse business incentives is a priority on the road to ensuring healthier online safety outcomes.
4. Therefore, CDH argues that this question is inversely framed.
5. The primary consideration is not what risks and costs are associated with tying senior manager remuneration to positive online safety outcomes, but rather what accountability it may provide to rectify the problems apparent in the present.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

## Service's risk assessment

### Question 7:

i) Do you agree with our proposals?

1. **Prioritisation system design over content decisions in service risk assessment** - CCDH is concerned that Volume 3, Chapter 9 "Service Risk Assessment Guidance" sets the wrong priority for services' risk assessment of illegal harms.
2. Section 9.3 states that the "illegal content risk assessment duties include a range of different elements. U2U services must assess the risk of users encountering priority illegal content or other illegal content by means of the service, and the level of risk that the service may be used for the commission or facilitation of a priority offence. They must **also** assess the nature and severity of the harm which may be suffered as a result" (CCDH-added emphasis).
3. System design considerations come *after* decisions about content and the likelihood of user encounters with illegal content. This is the wrong prioritisation.
4. This improper ordering is repeated in 9.4 where Volume 3 states "as part of the assessment, services must consider various characteristics of the service specified in the legislation – such as its user base, functionalities, business model, and systems and process – and **also** take into account of the relevant risk profile(s) produced by Ofcom" (CCDH-added emphasis).
5. Section 9.5 concerning search services and also places the requirement to "assess the nature and severity of the harm which may be suffered" *after* the requirement to consider encounters with illegal content.
6. Cumulatively, this prioritisation/ordering undermines safety by design and hardly encourages any upstream mitigations. Safety by design is not a siloed part of the Online Safety Act, but should permeate all areas of the regime, including here in service risk assessments.
7. **Avoiding tick-box assessment** - CCDH is concerned with the four-step risk assessment methodology described in Volume 3, table 9.2. The proposed matrix system makes regulatory reporting easier for services, but also risks becoming a tick-box exercise.
8. CCDH sees a tension between the holistic system proposed for risk management and governance systems in table 9.1 and the prescriptive nature of table 9.2. Recording risk assessments for an output, as by matrix in table 9.2, may not get to a holistic, self-reinforcing system pictured in table 9.1.
9. Specifically, table 9.2 is prescriptive because it does *not* require companies to do anything different to the Codes of Practice.
10. Positive-feedback loops that address systemic issues are rarely born from prescriptive tick-box processes.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

**Question 9:**

i) Are the Risk Profiles sufficiently clear?

1. As stated in our answer to question 1, the register or risks in Volume 2 was a strong rigorous assessment of the causes and impacts of illegal content and online harms. CCDH judges that the Volume 2 register of risks is a strong foundation for the risk profiles in Volume 3.
2. However, CCDH would raise the same concern as in question 7 (above): the need to prioritise systemic risks and risk profiles in services’ risk assessments.
3. The issue appears to be continual reference to the consideration of risk profiles and systemic issues as secondary to content judgements. Section 9.4 states that “as part of the assessment, services must consider various characteristics of the service specified in the legislation – such as its user base, functionalities, business model, and systems and process – and **also** take into account of the relevant risk profile(s) produced by Ofcom” (CCDH-added emphasis).
4. Further, 9.73 states that “Services are required to **take account** of our Risk Profiles when they carry out their risk assessments and given this, we consider their intended purpose is to help services conduct their risk assessment” (CCDH-added emphasis).
5. Finally, CCDH would note a disconnect between the evidence of harm presented in the risk profiles and the mitigation for those harms proposed in the Volume 4 codes of practice. The risk profiles identify systemic, overlapping risks and offences and should therefore be a fundamental consideration rather than something to be *taken account* of. The codes do not adequately address these aspects from the risk profiles and appear, to CCDH, to focus on content moderation choices and takedowns.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

**Question 11:**

i) Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?

Response: Yes

ii) Please provide the underlying arguments and evidence that support your views.

Response: N/A

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

## Volume 4: What should services do to mitigate the risk of online harms

### Our approach to the Illegal content Codes of Practice

#### Question 12:

i) Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?

1. CCDH believes the overarching approach to developing the illegal content Codes of Practice lacks focus on addressing systemic issues and ensuring safety by design.
2. CCDH believes the Codes contain overarching misalignment:
  - a. Recommending measures without describing desired outcomes
  - b. Not fully accounting for the register of risks in the Codes of Practice
  - c. Offering a safe harbour from enforcement, removing incentives for platforms to do anything beyond the measures prescribed
  - d. Over-reliance on “iterative” nature of the codes, establishing a weak baseline that will be harder to strengthen later on
3. **Recommending measures without describing desired outcomes** - the approach Ofcom has taken to developing the illegal content Codes of Practice has been to “set out measures we will recommend for services to comply with their safety duties” (11.2). Ofcom has interpreted the term “measures” as specific instructions, which is reasonable, but CCDH points out that “measures”, by definition, would **not** exclude describing desired outcomes.
4. The Act is clear: first and foremost, the onus sits with service providers to properly assess the risks users may encounter and decide which specific steps they need to take to address them (as referenced in “[Ofcom’s approach to implementing the Online Safety Act](#)”). A balance must therefore be found between the Act’s onus on the service providers to decide specific steps and Ofcom’s duty to assist platforms in compliance with their obligations. At present, CCDH believes the rules-based Codes do not strike the correct balance.
5. “Measures” do not need to be exclusively technical. As defined by the Online Safety Act in [section 236\(1\)](#), measures can be “any system or process” to comply with a duty of the Act. Safety by design being one of those duties, CCDH suggests incorporating a safety by design measure throughout the Codes to make them less prescriptive and more holistic.
6. **Not fully accounting for the register of risks described in Volume 2 in the Codes of Practice** - CCDH will expand on this in response to question 16 (below), but in general terms the the approach set out in Volumes 2 and 3 (identifying risks and the approach to risk management) does not follow through to the measures described in the Codes.
7. **Offering a safe harbour from enforcement** - CCDH is concerned with the potential consequences of offering a safe harbour from enforcement. As stated in Volume 4, 11.7: “Services that choose to implement the measures we recommended in our Codes of Practice will be treated as complying with the relevant duty. This means that Ofcom will not take enforcement action against them for breach of that duty if those measures have been implemented.”
8. CCDH fears that the combination of a tick-box list of measures in the Codes of Practice *with* a safe harbour provision against enforcement creates a perverse incentive for



regulated platforms to do the minimum necessary to tick-off the measures but do nothing further in the knowledge that they are safe from enforcement action.

9. Unaddressed, this combination could result in a situation where a service has flagged a particular risk within their risk assessment, such as a risk from a product design choice, but would not implement mitigating measures for this risk beyond what is described in the Codes – even if those measures are inefficient at mitigating that risk. Ofcom could then be prevented from taking enforcement action by the safe harbour protection in 11.7.
10. To address these risks, CCDH suggests Ofcom regularly revisit the enforcement safe harbour and conduct regular assessments of whether it is being misused by platforms.
11. **Over-reliance on “iterative” nature of the codes, establishing a weak baseline that will be harder to strengthen later on** – given the weaknesses CCDH highlights in the points above, CCDH is concerned that over-reliance on the iterative nature of these first codes will, in effect, establish a weak baseline for the regulatory regime that will be much harder to strengthen later on. Yes, it is true that the Codes can and will be updated. But it is critical that the first iterations are robust, setting a high bar to propel the future regulatory regime.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

### Question 13:

i) Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?

**Yes.** However, as answered in Questions 14 and 15, the definitions of “large” and “medium/high risk” services are currently too exclusionary. It is right that more onerous measures apply to large and risky services, but this necessitates better thresholds for what constitutes large and risky.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

### Question 14:

i) Do you agree with our definition of large services?

1. CCDH would point out a significant differentiation in Ofcom's approach to the risk assessment duties and the codes between large companies (7 million monthly users and above) and small companies (6.99 million and below).
2. CCDH believes the definition of “large” companies makes theoretical sense (and replicates a similar threshold as the EU DSA very-large platform status), but that this threshold is too high when in the context of the services operating in the UK. For example, services such as Fortnite or Roblox would not be caught up in this definition of “large service”. To contextualise, this would leave Roblox's [estimated 1.5 million](#) child users gaming on a platform with lower regulatory obligations. If large platforms like Fortnite and Roblox are not captured by the regime's definition of “large services”, that definition is too exclusionary.

<p>3. CCDH understands that additional "risky" status could catch smaller platforms and apply the same, more onerous obligations. Nevertheless, CCDH is concerned that the bar too high for what constitutes a "large", with large services having more online safety obligations, will thus exempt too many services from requirements CCDH would like to see broadly applied.</p> <p>4. Finally, it would be helpful to understand the legal basis upon which Ofcom has determined it is acceptable to use size as a factor in determining safety standards online.</p>
<p>ii) Is this response confidential? (if yes, please specify which part(s) are confidential)</p>
<p>No</p>

<p><b>Question 15:</b></p>	
<p>i) Do you agree with our definition of multi-risk services?</p>	<p>1. No. The proposed definition is that a multi-risk service is one that has "identified as medium or high risk for <u>at least two different</u> kinds of illegal harm in their latest illegal harms risk assessment" (underlined by CCDH).</p> <p>2. The threshold here is two different illegal harms, rather than the <i>medium</i> or <i>high</i> level of risk.</p> <p>3. CCDH would propose a risk-based threshold. At present, so long as a service had only <i>one</i> risk registered in their illegal harms risk assessment they would be exempt from the need to undertake more onerous mitigation measures, even if that risk was judged to be extremely high.</p> <p>4. This while a service with <i>two</i> medium risks - which could foreseeably be less risky together than a single extremely high risk - would be defined as "multi-risk" on the basis of the number of disparate harms rather than the riskiness of the harm or harm-level.</p> <p>5. CCDH would suggest the definition be amended so that even if it is a single instance, the severity of harm (the <i>high risk</i>) would require the extra obligations.</p>
<p>ii) Please provide the underlying arguments and evidence that support your views.</p>	<p>6. <a href="#">Changes</a> late in the Parliamentary passage of the Online Safety Bill allowed for category 1 designation to apply to companies on the basis of <i>either</i> size or risk. This brought small, high-harm services into scope of additional duties.</p> <p>7. CCDH would like to see the spirit of this change, broadening the application of mitigating measures and duties, reflected in the Codes and in the definition of "multi-risk" services.</p>
<p>iii) Is this response confidential? (if yes, please specify which part(s) are confidential)</p>	<p>No</p>

<p><b>Question 16:</b></p>	
<p>i) Do you have any comments on the draft Codes of Practice themselves?</p>	

1. The Codes lack focus on the Online Safety Act's duty to ensure "services regulated by this Act are *safe by design*" (Part 1.3.a).
2. The Codes suggest a process-driven approach that lacks outcome orientation. Their primary purpose is improving online safety by reducing illegal online content, **not** ensuring platforms meet their obligations under the Act. Platforms meeting their obligations is facilitatory towards the wider goal, not the goal in and of itself.
3. CCDH is concerned about the disconnect between the registered risks in Volume 2 and the mitigation measures proposed in the Codes of Practice in Volume 4.
4. The effect of this is to set the bar too low in terms of the measures with which regulated services must comply via the Codes and risks reinforcing the status quo which the legislation was intended to improve.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No

#### Question 17:

i) Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?

1. This is not a specific CCDH competency. But we would like to register that weighing public safety from illegal harms (grooming, terrorism, intimate image abuse etc) against costs to private companies (some worth billions of pounds) does not align with Parliamentary or public expectations of what the regulatory framework should achieve.
2. CCDH does recognise that costing is necessary for operating this regime. But as an organisation committed to rectifying the consequences these companies have had for individuals and society – all while they raked in massive profits – CCDH will reiterate that the cost to these companies is secondary to rectifying the harm they have done.
3. Finally, it is wrong to suggest that safety stifles innovation or competition. It is also wrong to suggest that if a small service is unsafe, the regulator should not take measures to address that lack of safety if those interventions could hinder the small platform's ability to compete.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

## Volume 5: How to judge whether content is illegal or not?

### The Illegal Content Judgements Guidance (ICJG)

#### Question 49:

i) Do you agree with our proposals, including the detail of the drafting?

1. CCDH believes that the illegal content judgement guidance could be strengthened by applying the systems-focused approach we suggest elsewhere in this consultation.
2. The guidance focuses on content assessment and whether or not it should be taken down. This does, of course, have basis in the Online Safety Act, but the guidance does not include the systemic language and proportionate system design obligations also contained in the Act.
3. CCDH is concerned with some aspects of the way Ofcom considers the burden of proof and weight of evidence in relation to illegal content judgements.
4. Ofcom seems to give preferential weighting to evidence collected from industry in many of the consultation documents, described as “best practice” from companies.
5. Choices about design should happen before you get the content flowing across the system and seen by users. This then defines the scope of Ofcom’s overall illegal harms approach, with an ex-post focus on measures, such as content moderation and take down.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No