Consultation response form

Please complete this form in full and return to IHconsultation@ofcom.org.uk.

Consultation Title	Protecting people from illegal harms online
Your Full Name	Stephen Tulip
Your Contact Phone Number	**0740653526**
Representing (Self or Organisation only)	Organisation
Organisation Name (if applicable)	**ACT | The App Association**
Email Address	stulip@actonline.org

Confidentiality

Is your name confidential? (please enter **yes** or **no** only)	**No**
Is your organisation name confidential? (please enter **yes** or **no** only)	No
Can Ofcom publish a reference to the contents of your response? (please enter **yes** or **no** only)	Yes
Please indicate if your full response is confidential. Partly confidential responses can be indicated under each question. (please enter **yes** or **no** only)	Yes

We ask for your contact details along with your response so that we can engage with you on this consultation. We will keep your contact number and email address confidential. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

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?
Response: ACT | The App Association strongly urges Ofcom to create an understanding and clear definition of these harms as acts or practices that cause or are likely to cause substantial injury to consumers. We strongly discourage 'likely to be permitted' language, meaning 'possible', which could attach legal liability to commercial activity based on under-demonstrated and/or theoretical harms. The App Association believes that Ofcom should not deem an act or practice harmful unless it is injurious in its net effects, and that any HM Government agency or agencies implementing such a law enact this innovation- and consumer-friendly approach. The App Association therefore generally agrees that Ofcom's categorisation of harms into 15 proposed categories comprehensively captures causes of online harms, noting our support for Ofcom's mapping of defined online harms to approximately 130 priority offences defined in the Act, as such a scoping aligns with our recommendation that defined harms be substantiated with evidence and legal bases.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: The App Association appreciates Ofcom's rigorous analysis, which will ensure that HM Government does not pursue hypothetical injuries in a manner that will hinder small businesses' investment and innovation. We encourage maximum alignment with ISO 31000, *Risk management – Guidelines* (https://www.iso.org/iso-31000-risk-management.html) and other international standards that provide standardised principles, frameworks, and processes for managing risk. The App Association notes its significant concern with Ofcom's characterisation of end-to-end encryption as a 'functionality' posing 'particular risks'. Our members are at the forefront of innovation, practicing responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, utilising the most advanced technical protection mechanisms (e.g. end-to-end encryption) is a market-driven necessity. Consumers depend on our members to keep their valuable data safe and secure, therefore, maintaining consumer trust is the bedrock of our members' triumphs. Should HM Government mandate vulnerabilities in encryption in an attempt to address online harms, it will create backdoors intended for law enforcement that will be exploited by criminal enterprises and nation-state backed hackers, leading to substantially more harm to consumers. With respect to 'recommender systems', it is important to differentiate between pro-competitive systems and those that can cause harm by repeatedly distributing harmful content. Recommender systems are themselves not harmful and can in fact lead to greater efficiency, better quality, or	

lower costs for consumers. Such systems are not harmful and further, there are minimal antitrust issues when users can easily switch to another platform. We do however support the ambition to protect vulnerable people from harm by preventing the recommendation and repetition of harmful content. HM Government should expect competition to discipline examples where recommender systems are harming consumers because those consumers can leave the platform due to demonstrably low switching costs. Unfortunately, in other jurisdictions such as the European Union (EU), policymakers have proposed flipping the burden onto recommender systems to show that such systems have no long-run harmful effects; the App Association discourages such an approach elsewhere because (1) recommender systems should not be unfairly forced to prove a negative when accused of causing harm and (2) it would chill market activity that widely benefits consumers.

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

Response: Yes, all.

Question 2:

i) Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.

Response: Generally, we encourage maximum alignment with ISO 31000, *Risk management – Guidelines* (https://www.iso.org/iso-31000-risk-management.html) and other international standards that provide standardised principles, frameworks, and processes for managing risk.

Specific concerns we have with Ofcom's proposals include:

- The App Association notes its significant concern with Ofcom's characterisation of end-to-end encryption as a 'functionality' posing 'particular risks'. Our members are at the forefront of innovation, practicing responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, utilising the most advanced technical protection mechanisms (e.g. end-to-end encryption) is a market-driven necessity. Consumers depend on our members to keep their valuable data safe and secure, therefore, maintaining consumer trust is the bedrock of our members' triumphs. Should HM Government mandate vulnerabilities in encryption in an attempt to address online harms, it will create backdoors intended for law enforcement that will be exploited by criminal enterprises and nation-state backed hackers, leading to substantially more harm to consumers.
- With respect to 'recommender systems', it is important to differentiate between pro-competitive systems and those that can cause harm by repeatedly distributing harmful content. Recommender systems are themselves not harmful and can in fact lead to greater efficiency, better quality, or lower costs for consumers. Such systems are not harmful and further that there are minimal antitrust issues when users can easily switch to another platform. We do however support the ambition to protect vulnerable people from harm by preventing the recommendation and repetition of harmful content. HM Government should expect competition to discipline examples where recommender systems are harming for consumers because those consumers can leave the platform due to demonstrably low switching costs. Unfortunately, in other jurisdictions such as the

	European Union (EU), policymakers have proposed flipping the burden onto recommender systems to show that such systems have no long-run harmful effects; the App Association discourages such an approach elsewhere because (1) recommender systems should not be unfairly forced to prove a negative when accused of causing harm and (2) it would chill market activity that widely benefits consumers.
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

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?
Response: The App Association appreciates Ofcom's proposed approach which scales risk to large and/or multi-risk services, which is appropriately aligned with harm-proportionate risk management practices captured in international standards noted above. Ofcom's proposed approach to governance and accountability measures in the Codes of Practice for illegal content are generally flexible and scalable (and aligned with leading international risk management standards noted above), permitting tailored approaches to consumer protection as necessitated by specific use cases. Therefore, we generally support Ofcom's proposals that would ensure the use of a risk-based approach and proportionality in complying with governance and accountability requirements. We appreciate Ofcom's tailored proposals that recognise that small companies (like the App Association's members) have limited resources and avoid taking an approach that will suppress the UK's digital economy startups and small businesses (to the advantage of larger incumbents) and unduly limit access to digital economy startups and small business innovations from abroad, ultimately damaging the public interest. We agree with Ofcom's decision to not yet make any recommendations regarding external audit requirements, or regarding linking remuneration and bonuses to online safety outcomes due to limitations in currently available evidence.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: Generally, no. We recognise and appreciate Ofcom's efforts to ensure that its proposed governance and accountability do not unhelpfully duplicate or somehow contradict existing governance and accountability requirements in other laws or typical approaches taken aside from legal compliance.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?

Response: Yes.
ii) Please explain your answer.
Response: Ofcom has provided clear definitions of in-scope services (user-to-user services, search services, and services that feature provider pornographic content).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 5:
i) Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response: No.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

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?
Response: The App Association questions whether regulating the renumeration of senior managers is an optimal means of accomplishing HM Government's goals and is concerned with the precedent such an intervention might set.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Service's risk assessment

Question 7:
i) Do you agree with our proposals?
Response: The App Association generally supports Ofcom's proposed four-step risk assessment and Risk Profiles, and requests maximum alignment with standardised risk management approaches referenced above.
ii) Please provide the underlying arguments and evidence that support your views.

Response: See ISO 31000, *Risk management – Guidelines* (https://www.iso.org/iso-31000-risk-management.html)
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:
i) Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response: The App Association generally supports Ofcom's proposed four-step risk assessment and Risk Profiles, and requests maximum alignment with standardised risk management approaches referenced above.
ii) Please provide the underlying arguments and evidence that support your views.
Response: See ISO 31000, *Risk management – Guidelines* (https://www.iso.org/iso-31000-risk-management.html)
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response: Generally, yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response: Yes, the information provided on risk factors will improve understanding of the risks on a service.	
iv)	Please provide the underlying arguments and evidence that support your views.
Response:	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: We urge Ofcom to ensure that its burdens placed on small businesses are kept to a minimum. In taking a scaled approach to risk management, Ofcom's proposals largely do this. However, we urge for continued examination for ways to ensure that small businesses are not unduly burdened with record keeping and other administrative requirements.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

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:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

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?
Response: Generally, we expect the Codes of Practice to foster a culture of compliance by providing an easily understood roadmap that may be used for self-assessments. We appreciate alignment with widely relied upon scaled risk management practices captured in international standards (referenced above).	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

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?
Response: Yes. To do otherwise would depart from scaled risk management approaches that ensure measures taken are proportionate to harms, which the App Association would strongly oppose.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: HM Government's approach to addressing online harms should be flexible and scalable, permitting tailored approaches to consumer protection as necessitated by specific use cases. Therefore, we support Ofcom's proposal to ensure the use of a risk-based approach and proportionality in regulatory practice. App Association members have limited resources and are unable to spend the large amounts of money on outside counsel and consultants that larger companies can access. Should HM Government take an approach that is too rigid, it will suppress the UK's digital economy startups and small businesses to the advantage of larger incumbents and unduly limit access to digital economy startups and small business innovations from abroad, ultimately damaging the public interest.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 14:	
i)	Do you agree with our definition of large services?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.

Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 15:
i) Do you agree with our definition of multi-risk services?
Response: Yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 16:
i) Do you have any comments on the draft Codes of Practice themselves?
Response: Generally, we expect the Codes of Practice to foster a culture of compliance by providing an easily understood roadmap that may be used for self-assessments. We appreciate alignment with widely relied upon scaled risk management practices captured in international standards (referenced above).
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

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?
Response: No.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: Generally, yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Content moderation is a necessary, complex, and unending task that operators of online services willingly undertake to maintain functioning online communities. Online services try to remove harmful and objectionable content as quickly as possible—ideally before many (if any) people see it. They rapidly determine whether submitted content is so objectionable that it should be removed under the online services' policies or whether there is a way to effectively reduce the content's spread. Succeeding at content moderation therefore requires a continuous,

iterative process of improvement. The global internet's sheer scale and the complexities of human interaction (in all languages and across many cultures) complicate online services' efforts. Online services have become able to quickly and effectively parse individual pieces of content's context to determine whether and how to continue disseminating that content. Online services may determine that not all potentially harmful content warrants removal and, conversely, not all policy-compliant content is worthy of prominent presentation. And there will not always be 'correct' answers about how to address specific content. We are supportive of Ofcom's U2U content moderation proposals that provide needed flexibility for such good faith moderation activities.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Content moderation (Search)

Question 19:
i) Do you agree with our proposals?
Response: Generally, yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Content moderation is a necessary, complex, and unending task that operators of online services willingly undertake to maintain functioning online communities. Online services try to remove harmful and objectionable content as quickly as possible—ideally before many (if any) people see it. They rapidly determine whether submitted content is so objectionable that it should be removed under the online services' policies or whether there is a way to effectively reduce the content's spread. Succeeding at content moderation therefore requires a continuous, iterative process of improvement. The global internet's sheer scale and the complexities of human interaction (in all languages and across many cultures) complicate online services' efforts. Online services have become able to quickly and effectively parse individual pieces of content's context to determine whether and how to continue disseminating that content. Online services may determine that not all potentially harmful content warrants removal and, conversely, not all policy-compliant content is worthy of prominent presentation. And there will not always be 'correct' answers about how to address specific content. We are supportive of Ofcom's U2U content moderation proposals that provide needed flexibility for such good faith moderation activities.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Automated content moderation (User to User)

Question 20:
i) Do you agree with our proposals?
Response: Generally, yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: Content moderation is a necessary, complex, and unending task that operators of online services willingly undertake to maintain functioning online communities. Online services try to remove harmful and objectionable content as quickly as possible—ideally before many (if any) people see it. They rapidly determine whether submitted content is so objectionable that it should be removed under the online services' policies or whether there is a way to effectively reduce the content's spread. Succeeding at content moderation therefore requires a continuous, iterative process of improvement. The global internet's sheer scale and the complexities of human interaction (in all languages and across many cultures) complicate online services' efforts. Online services have become able to quickly and effectively parse individual pieces of content's context to determine whether and how to continue disseminating that content. Online services may determine that not all potentially harmful content warrants removal and, conversely, not all

policy-compliant content is worthy of prominent presentation. And there will not always be 'correct' answers about how to address specific content. We are supportive of Ofcom's U2U content moderation proposals that provide needed flexibility for such good faith moderation activities.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 21:
i) Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response: No.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Do you have any relevant evidence on:

Question 22:
i) Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response: No.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 23:
i) Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response: No.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We agree with Ofcom's characterisation of hash matching and the difficulties smaller entities would face due to the limited number of providers of relevant databases and their capacity.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 24:

i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response: No.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: We agree with Ofcom's characterisation of the costs of applying CSAM URL detection measures to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response: No.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: We agree with Ofcom's characterisation of the costs of applying Ofcom's articles for use in frauds (standard keyword detection) measures, including for smaller services.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.
Response: No.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: We agree with Ofcom's characterisation of the effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and the costs and efficacy of applying hash matching and URL detection for terrorism content.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Terms of service and Publicly Available Statements

Question 29:
i) Do you agree with our proposals?
Response: Yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 30:
i) Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: No.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Default settings and user support for child users (U2U)

Question 31:
i) Do you agree with our proposals?
Response: Partially.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Mandates to limit access to sensitive content by default may introduce an overly burdensome layer of complexity and exceed some small companies' budgets. Protecting children's privacy and providing them with a positive, safe online experience are worthy and widely shared goals, but age verification is a complicated enterprise. Companies, particularly when dealing with internet-savvy children, are afforded little confidence when users assert that they are of appropriate age by checking a box or provide proof using, for example, government-issued identification that can easily be falsified. New technologies available to verify children's age or age range may afford companies with greater assurance. These tools also benefit companies by helping them comply with laws and guidance designed to protect children from other harms online. With greater certainty about the user's age or age range, companies are better able to prevent children from accessing

inappropriate material and to direct them to more suitable online content and activities. They are also better equipped to keep adults out of online environments intended for children.

But more rigorous, reliable solutions may involve the use of data and methods that raise their own privacy issues for children. While data about a child's birth date, family background, or academic record could verify age with a high level of certainty, the privacy implications of gathering and processing such data are clear. Use of biometric data, such as retinal or iris scan, voiceprint, or facial image, may heighten these concerns. And the potential long-term storage of data about children and its sharing with third parties for secondary purposes raises concerns about creation of stores of data that could be misused or processed in ways that could cause them harm.

We urge Ofcom to ensure its efforts to protect minors online align with the following recommendations:

- Any requirements for age verification must be sufficiently flexible to ensure that they are applied in a manner proportional to the risk data collection poses for children. How rigorous age verification should be—and therefore the amount and kind of data needed to accomplish it —must be tailored to the degree of certainty necessary to protect children.
- Laws and regulations should provide for periodic review of age verification technology solutions to make sure they are applied only where necessary for compliance and to identify how they might be refined to scale certainty to risk. They should also provide incentives for developers to continue to develop new approaches that optimise privacy. Incentives should also promote development of solutions that minimise the data required to establish a child's age or age range – and encourage its disposal after age verification occurs.
- Laws and regulations should place age verification in the context of privacy by design. While ensuring that children are of legal age to consent to data collection is important, building into the design of interfaces and technologies greater transparency and privacy-enhancing practices may mitigate the risk posed by the collection of children's data and minimise the need for age verification that potentially compromises privacy.

With the right safeguards in place, children can enjoy an online experience that protects all aspects of their data privacy. HM Government should take steps to ensure that age verification and children's privacy is not a zero-sum game.

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

Response: Yes, all.

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?

Response: No.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 33:
i) Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response: No.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Recommender system testing (U2U)

Question 34:
i) Do you agree with our proposals?
Response: Yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Question 35:
i) What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response: We support HM Government's development of easily understood codes of conduct that may be used for self-assessments. Furthermore, we reiterate our support for HM Government encouraging companies, particularly the digital economy's small businesses that the App Association represents, to attest to and document adherence to this code of conduct, in return receiving a safe harbour from liability under related online harms laws and regulations.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:

i)	Are you aware of any other design parameters and choices that are proven to improve user safety?
Response: No.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: We urge for maximum flexibility on how controls are made known to users to permit U2U services to develop optimal user interfaces (and to evolve them with user preferences that evolve over time).	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response: We are unsure.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response: Yes.	

ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response: We have no further supporting information or evidence to provide.	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response: We have no further supporting information or evidence to provide.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 42:	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response: We have no further supporting information or evidence to provide.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response: We have no further supporting information or evidence to provide.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The App Association appreciates Ofcom's measures proposed to support low risk small and micro businesses, consistent with our views shared above.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?

Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response: Yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

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?
Response: Generally, yes.	
ii)	What are the underlying arguments and evidence that inform your view?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: Generally, yes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response: We generally agree with Ofcom's assessment.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:
i) Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response: Yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We request that the information gathering process keep burdens on small businesses to a minimum, while fully respecting the need for such a process.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Enforcement powers

Question 53:
i) Do you have any comments on our draft Online Safety Enforcement Guidance?
Response: Yes.
ii) Please provide the underlying arguments and evidence that support your views.
Response: We offer the following general views: • The App Association strongly supports HM Government providing as much clarity as possible regarding enforcement. We believe this information should be provided in a clear and easily understood manner in accessible formats. • HM Government should foster a culture of compliance by providing an easily understood code of conduct that may be used for self-assessments. Furthermore, we urge HM Government to encourage companies, particularly the digital economy's small businesses that the App Association represents, to attest to and document adherence to this code of conduct, in return receiving a safe harbour from liability under related online harms laws and regulations. • We discourage HM Government from creating mandatory certifications that would be conducted by third parties. Such certifications are often expensive and will unduly drain resources from digital economy small businesses when larger companies would experience a net benefit due to being able to absorb such costs. • We strongly urge HM Government to ease the path to compliance for those that may find themselves facing liability with regard to this new duty of care for online harms. For example, HM Government should ensure that any company accused of violating new online harms rules be afforded an informal remediation avenue before formal

enforcement proceedings are initiated. This informal period will save our small business members from expensive and unnecessary legal fees.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response: We have no view on this question.	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response: N/A.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: Yes, all.	