Consultation response form

techUK Illegal Harms Consultation Written Response

techUK is submitting a written response to Ofcom's Illegal Harms Consultation. techUK is the trade body for digital tech in the UK, representing over 1000 members. Our membership is made up of a range of companies which include some of the services and platforms which are within scope of the Online Safety Act. Many of these companies work across borders and therefore, it is vital that Ofcom continues collaborating with global regulators to encourage multilateral standards that combat online harms effectively. While we have responded to each question directly via the online form, there are some additional points which are important to raise below.

TechUK acknowledges the extensive nature of the consultation materials, spanning over 1,700 pages of guidance. While we endorse the consultation objectives and understand the importance of comprehensive engagement from the regulator, the challenge of achieving representativeness when a response requires enormous resource allocation must be highlighted. This is especially due to the potential in limiting the diversity of perspectives represented.

Additionally, we recognize the concerns raised by our members regarding the potential volume of guidance and codes that may follow this consultation. If the extensive nature of the consultation document is indicative of the length of the likely guidance and codes, this could pose challenges for companies striving to comply but lacking the resources to digest and interpret such comprehensive guidance. While this concern is addressed at Q50, we recommend elevating its priority in the consultation process to better address the potential practical challenges faced by companies in implementing Ofcom's guidance.

We recommend that Ofcom streamline its approach to enhance accessibility and reduce barriers at the compliance stage, especially for SMEs that may face challenges due to limited resources and legal expertise. Ofcom has a duty for proportionality within the OSA. Emphasizing proportionality and usability in issuing guidance will contribute to a more effective and widespread implementation of the proposed measures, ensuring that smaller or lower risk entities can navigate the obligations without undue burden. TechUK looks forward to collaborating with Ofcom to ensure that the guidance is practical and navigable for a diverse range of services, including those with limited legal expertise and resources.

Clarity on Definitions

We stress the paramount importance of providing clarity on essential terms and definitions within the consultation. Ensuring a common understanding, particularly for terms like ‘large services,’ ‘low risk,’ and ‘multi risk,’ is imperative for effective implementation and enforcement. This is alongside clarity on the differences between ‘high risk’ harm versus ‘low risk harm’. Moreover, it is crucial to draw attention to the need for flexibility in the definition of 'user.' While Ofcom has indicated that the “average user base… per month in the UK” will be the basis for determining if a service is “large,” we advocate for acknowledgment that companies are best positioned to understand how their customers use and interact with the service. Therefore, they should be allowed to apply the most appropriate calculation of size, taking into account available data on use and access, to address risk effectively.

The Importance of Flexibility for Services

As highlighted in our answers, avoiding a one-size-fits-all approach, maintaining flexibility, and adopting a proportionate stance based on the nature and size of services will be vital. It is noteworthy that the OSA considered the importance of different business models and that it intended not to regulate Business to Business services, as was made clear in Parliament.

Continued nuance will be vital and will involve adopting a risk-based approach that considers the unique challenges faced by different types of services. For example, it’s commendable that the functionality and proliferation of U2U content is considered when determining the risk level of a service. However, there should be more nuance to make this more targeted, especially when U2U content is ancillary to the core purpose of the wider service. Compliance measures should also not be disproportionate to the limited risk associated with a specific part of a service's functionality.

There is also a need for flexibility in risk assessment, allowing companies to tailor assessments to their specific business models. While the processes prescribed in Ofcom’s guidance may be helpful for some businesses, in general the approach is overly prescriptive and it will limit the ability of more established businesses to align risk assessment processes under the Act with existing good practice risk management processes. Some businesses will have multiple services in scope, each different in nature and operating with distinct business models. Acknowledging this diversity is crucial to ensuring that compliance measures remain adaptable to the varying operational realities of different service providers.

Furthermore, flexibility will be essential concerning the practicality and potential burden of record-keeping duties, ensuring they align with the operational realities of different service providers. Striking a balance between effective regulation and accommodating the diversity of services will be key to fostering innovation and responsible digital practices within the tech industry.

Impact on Smaller Services

techUK welcomes the recognition that providers of smaller in-scope services are positioned differently, especially when provided by SMEs, and that the application of the OSA should be adapted accordingly for a proportionate framework.

A thorough impact assessment of the proposed measures, particularly on smaller and lower risk services, will be necessary to give effect to this objective and understand the potential challenges and costs for this category of services. For example, the immense governance burden that compliance could inadvertently place on SMEs. This concern aligns with our previous comment on the size of consultations and guidance. Specifically, this assessment should delve into:

- The expected volume and frequency of interactions between Ofcom and the provider of a smaller in-scope service.
- The burden, proportionality, and feasibility of conducting annual reviews.
- Whether a named person accountable for compliance is essential for smaller services.
- The resources needed for training requirements for staff.
- The resource allocation for content moderation and the potential impacts on service quality.

To strengthen the effectiveness of the regulatory framework, Ofcom should seek to streamline its approach, minimizing barriers to adoption, and ensuring guidance is issued with a focus on proportionality and usability. This will not only benefit SMEs but will also contribute to the overall effectiveness and inclusivity of the regulatory framework.

Role of Industry Engagement and Collaboration

In recognition that online harms experienced by users transcend geographical boundaries, global collaboration between Ofcom, global regulators and the tech industry is paramount to developing realistic and effective best practices and guidelines. techUK strongly advocates for continued and meaningful engagement between Ofcom and industry to encourage practical solutions aimed at reducing user harms, including mutual recognition of guidelines and standards among global regulators.

Industry collaboration is critical at this stage for several reasons, most importantly to ensure that the scope of application of OSA rules is clearly in line with the requirements of Schedule 4 and reflects the overarching intent of the Act. It will be important for Ofcom to make time and safe space for this stage before finalising codes and be open to making further adjustments in the light of this consultation. Engagement is also vital in order to develop workable and effective best practices and guidelines for all providers of in scope services. An iterative process which considers evolving technologies and online risks, is crucial for the development of a regulatory

framework that stands the test of time. We look forward to ongoing collaboration to address these challenges and build a safer online environment.

Implementation timeline

We urge Ofcom to grant services adequate time for implementing their guidance. We believe that ensuring services have ample time is crucial for fostering voluntary compliance. While we appreciate Ofcom's comprehensive guidance, including annexes, it requires thorough analysis post-finalization. We understand that Ofcom's implementation roadmap may change, especially due to the upcoming general election. Presently, the roadmap indicates platforms must implement guidance upon parliamentary approval and we suggest that Ofcom should review these timelines in light of the length and complexity of the guidance.

***

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?
While understanding the need for effective moderation, we emphasize the challenges associated with real-time content moderation for some services. Striking a balance between mitigating online harms and preserving user freedom is crucial. A collaborative approach with the industry can help find practical and effective solutions that do not unduly burden platforms. Having less prescriptive content moderation practices will allow platforms to implement solutions that are more effective in addressing illegal content while accounting for their level of risk, business model and nature of their content. Evidence Base The evidence referenced in Vol. 2 forms the basis of Ofcom's register of risks, which companies are expected to have reference to when carrying out their own risk assessments. We therefore agree with Ofcom that it is important to take steps to ensure that evidence sources for these risks are robust and reliable. As part of the consultation, Ofcom have asked services whether they have comments on Ofcom's assessment of the causes and impacts of online harms. We have noted instances where Ofcom have relied on evidence which has previously been questioned by peers. It would therefore be helpful to understand Ofcom's approach to selecting evidence sources, and the steps that have been taken to ensure that these are robust and reliable. TechUK advocates for any evidence base or research Ofcom seeks to rely upon to be in line with Ofcom's own rules for research, and have a published methodology and peer review. Some of the research cited in Volume 2 has cited evidence that is either out of date and no longer reflective of the market or harms, is inaccurate or has a poor methodology or lacks the relevant evidence altogether, in relation to the measures proposed.
ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Some providers may not be clear as to whether their services are in scope and the analysis omits to explain how providers will acquire certainty in this regard. TechUK recommends that Ofcom creates further time and safe space to complete this step before finalising codes, carrying out additional targeted consultation where needed.

TechUK rejects the proposal that Ofcom publicly 'name and shame[1]" providers as a lever to secure compliance. While techUK members expect Ofcom to publish formal enforcement decisions, they also expect the day-to-day operation of the online safety framework and Ofcom's conduct to match the aspirations previously set out. techUK asks that Ofcom establish a clear and predictable hierarchy of interventions from the outset, consistently starting with direct engagement with a provider and driving towards workable compliance that addresses identified risks.

In addition, Ofcom should adopt a 'no surprises' approach to research by publishing its programme and providing reasonable opportunities for relevant providers to comment before research is commissioned. This will give effect to the collaborative approach Ofcom has presented, avoid Ofcom resources being wasted on flawed or misleading research and build trust between Ofcom and regulated companies.

More generally, TechUK suggests a continuous dialogue between regulators and the tech industry to address emerging challenges promptly. Collaboration and shared insights, even with similar international regimes, can enhance the effectiveness of the proposed measures

Finally, it is important to highlight the benefits of encryption to public safety and security. TechUK welcomes Ofcom's acknowledgment that encryption plays a vital role in keeping communications safe and secure. We urge Ofcom to make a stronger and more explicit statement in this section, especially considering their recognition of encryption as a 'particular risk' when used on services. Highlighting the benefits of encryption is essential for maintaining a balance between privacy and security concerns, and it is imperative that Ofcom's position reflects the positive contributions encryption makes to public safety.

[1] "....using our research and our transparency reporting powers to shine a light on what services are doing to tackle online harms and generating reputational incentives for them to make improvements", p6

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

No

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.

TechUK encourages a nuanced understanding of risk factors, considering the diversity of tech services. The risk assessment framework should be flexible to accommodate various business models and service types. End to end encryption

for example, is described as 'high risk'. However, E2EE needs to be considered with all the benefits it brings in reducing other illegal and harmful online harms in mind. Similarly, for artistic content, a more nuanced approach is needed to balance the protection of users with the preservation of artistic freedom and freedom of expression

Further, when making an assessment on harm, it is vital that the risk and type of harm is factored in and mitigation measures that would reduce risk are effectively considered. The scale and focus of services' prioritisation and mitigation measures should be taken into account.

Additionally, Ofcom should reserve the most significant obligations for services with the highest risk of harm. We are concerned current draft proposals could lose sight of the OSA's emphasis on risk and proportionality, and instead adopt an approach which has an undue focus on size.

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

Response: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?
TechUK supports the importance of governance and accountability. However, we propose flexibility in the implementation, recognizing the diverse nature and sizes of tech companies. A one-size-fits-all approach may affect the diversity of content and user expression. Many platforms regulated by Ofcom operate cross-border, meaning their governance arrangements may not be UK-specific. We encourage Ofcom to collaborate with global regulators to promote consistent global governance standards that effectively combat user harm, while also paying attention to the limits of powers granted by UK parliament. The Code of Practice should offer guidance, while allowing services flexibility in compliance while ensuring a safer online environment. Ofcom must also take a proportionate approach to illegal harms, including allowing services to prioritise certain harms and offences over others, depending on the nature of the service. On content moderation, Ofcom should factor in that each moderation approach is likely to have different timescales. Certain content-moderation decisions, for example those regarding artistic or political content, require a thoughtful and deliberative approach, including the solicitation of advice from third-party experts. Different content types also have different review timelines, for example a podcast takes much longer to review than an image. We also caution against Ofcom's desire to penalise "excessively" fast decision-making where an appropriate risk-based approach has been followed.
ii) Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
TechUK suggests further consideration of the scalability and practicality of proposed measures, ensuring they align with the operational capacities especially of smaller or lower risk tech companies.

Given the size, scope and complexity of the regulation, we ask that guidelines are harmonised as far as possible with the EU's Digital Services Act to avoid conflicting standards or excessive compliance costs for lower risk services.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 4:
i) Do you agree with the types of services that we propose the governance and accountability measures should apply to?
TechUK advocates for a risk-based approach to determine the types of services subject to governance measures. Consideration should be given to the potential impact on smaller or innovative services.
ii) Please explain your answer.
TechUK recommends a tiered approach, tailoring measures based on the size and nature of services, to avoid disproportionate burdens on smaller tech companies.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

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?
As representatives of a diverse range of tech companies in scope of the Online Safety Act, we wish to express our reservations about the necessity and implications of such measures. Privacy Concerns: While we recognize the importance of ensuring a safe online environment, we must also acknowledge the significant privacy concerns associated with external audits of content moderation measures. Tech companies handle vast amounts of user data, and subjecting these processes to third-party audits raises concerns about the confidentiality and protection of user information. Any auditing mechanism must be

designed with robust privacy safeguards to prevent unauthorized access and ensure compliance with data protection regulations.

Internal Audit Functions Adequacy:

Our member companies widely employ robust internal audit functions that are sufficiently independent and effective in assessing and managing risks, including those related to illegal content. These internal processes are tailored to the specificities of each platform and are designed to ensure compliance with online safety standards.

Risk of Talent Deterrence:

Imposing mandates for external audits may inadvertently discourage top-tier talent from joining the industry. The tech sector is highly competitive, and executive recruitment efforts are already challenging. Such stringent measures could hinder the sector's ability to attract and retain the best minds in the field. If we don't have the top minds, we are as a result limiting not only innovation but also safety.

Balancing Accountability and Innovation:

We believe in the importance of holding platforms accountable for user safety. However, a flexible approach is essential to foster innovation. Mandating external audits may lead to a one-size-fits-all approach that fails to consider the varied business models and risk profiles within the tech industry.

Collaborative Industry Involvement:

Instead of relying solely on external audits, we propose increased collaboration between industry stakeholders and regulators to develop effective self-assessment frameworks. This approach ensures a dynamic and adaptive response to emerging risks while maintaining a healthy balance between accountability and innovation.

TechUK suggests a collaborative exploration of audit mechanisms, considering the feasibility and cost implications for tech companies. A phased approach may be appropriate for different service sizes

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

Response: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?

TechUK recommends a cautious approach to linking remuneration with online safety outcomes. While recognizing the importance of aligning incentives with

positive safety outcomes, it's crucial to establish a transparent and fair framework. This framework should avoid unintended consequences and encourage responsible innovation. Such proposals should also be subject to specific consultation which can consider related factors such as providers' freedom to do business, each services' varying processes and metrics which effect their measurement of safety outcomes, and the acquisition and retention of high quality leadership in the tech industry.

TechUK looks forward to engaging in further discussions with Ofcom to define a balanced and effective system that promotes online safety without stifling the creativity and dynamism of the tech industry. TechUK would strongly advise against having in scope services take overly intrusive approaches in order to get better online safety outcomes, if this is to the detriment of user privacy or freedom of expression.

TechUK highlights that it is vital to focus on prioritisation here. This is the first code, and the focus should be on how we can tackle illegal harms, rather than to call for evidence of a measure that has unclear enforcement and is vague on the specifics of the proposal.

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

Response: No

Service's risk assessment

Question 7:

i)	Do you agree with our proposals?

TechUK welcomes Ofcom's statements in the opening paragraphs of Volume 3 which note that '*there is no one size fits all [to risk assessments]*'(Vol. 3, para. 9.24), and that Ofcom have therefore adopted '*a scalable approach [to risk assessments] which allows services to differentiate based on their size, nature and likely levels of risk*' (Vol. 3, para 9.36). In our view, flexibility is crucial to ensure that Ofcom's guidance can work for a diverse range of business models, and that it can support evolving technologies and risks.

We note, however, that there are sections, such as Volume 3 and Annex 5 where the prescriptive nature of the guidance means that it is difficult in practice to see how companies may be able to adopt a flexible approach. TechUK would therefore invite Ofcom to consider the tension between proposing companies flexibly meet their risk assessment obligations under the Online Safety Act whilst also proposing prescriptive guidance.

Further, the draft risk assessment guidance does not clearly distinguish between inherent (i.e. before risk mitigation measures) and residual (i.e. after risk mitigation

measures) risk, which means that the adequacy of existing compliance measures may not be taken into account when the draft codes recommend further compliance measures.

We are also asking Ofcom to recognize in its Risk Assessment Guidance that where the creation of user-generated content is ancillary to the core purpose of the service, then that minimizes the risks posed by any illegal content that may be present on the ancillary part of the service.

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

TechUK emphasizes the need for continuous dialogue between regulators and each provider of an in-scope service to refine risk assessment processes based on real-world challenges and technological advancements. All in-scope services are entitled to expect the application of online safety regulation to reflect their individual risk assessment, without over-generalisation or conflation with other services Ofcom may understand better.

A critical aspect of this dialogue is the necessity for a clear and transparent risk assessment framework. The current uncertainty surrounding which services are in scope and the specific duties for individual organizations creates significant confusion for tech services and makes it difficult for them to understand their duties.

It is imperative to establish a well-defined risk assessment process that outlines which services fall within the regulatory scope and clearly delineates the duties imposed on each service. Clarity in these aspects is essential for service providers to understand and effectively apply the legislation, fostering compliance and accountability across the industry. TechUK recommends a collaborative effort to establish a transparent risk assessment mechanism that provides clear guidelines for both regulators and tech companies, ensuring a fair and effective implementation of the legislation.

As mentioned above, our view is that the guidance on when services are required to update their assessments is too inflexible. For example, Ofcom have provided guidance on when companies may be required to update their risk assessments in accordance with s.9(4) of the Online Safety Act. In particular, Table 13 of Annex 5 provides the following guidance on what is likely to constitute a 'significant' change:

- *The proposed change alters the risk factors which you identified in your last risk assessment.*
- *The proposed change impacts a substantial proportion of your user base or changes the kind of users you expect to see on your service.*
- *The proposed change impacts a vulnerable user group, such as children.*

- *The proposed change impacts the efficacy of the measures you have put in place following your last assessment to reduce the risk of illegal content appearing on your service.*
- *The proposed change impacts your revenue model, growth strategy and/ or ownership in a way that affects its service design.*

This guidance could be interpreted to suggest that services are required to update their risk assessments in the case of almost any change to the design or operation of their service, which would seem at odds with Ofcom's opening statements in Volume 3 (and with a common sense interpretation of the word 'significant'). For example, a platform may make a minor change to their community guidelines which would necessarily impact a substantial proportion, if not all, of its user base.

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

No

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?

TechUK acknowledges the usefulness of the proposed models. However, ongoing collaboration is essential to refine these models and ensure they remain effective and adaptable.

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

TechUK suggests regular feedback mechanisms to refine the risk assessment process based on industry insights and changing technological landscapes.

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

No

Question 9:
i) Are the Risk Profiles sufficiently clear?
TechUK recommends clarity in Risk Profiles, with continuous industry engagement to enhance understanding and interpretation. As noted above, Ofcom must take steps to avoid damaging over-generalization or bias based on its understanding of the services it already knows well. We express concern that the current drafts may be too broad and lack nuance. For example, the assessment that end-to-end encryption (E2EE) increases the risk of illegal harms such as fraud. It is important to bear in mind that E2EE provides additional protections that actually reduce the risk of fraud by ensuring secure communication channels. For example, there is literature that E2EE in RCS messages can lead to a reduction in a wide variety of fraudulent activities such as impersonation and malware attacks. Furthermore, we disagree with the broad categorization of all file-sharing and file storage sites as high risk. This approach overlooks crucial distinctions between different types of services. Judging all file-sharing and storage services as high risk solely because they allow the functionality of uploading images, and subsequently subjecting them to recommendations to scan, is disproportionate and could negatively impact most users of these services who utilize them for entirely innocent means. Categorizing all file-sharing and file storage sites in the same manner is too simplistic and may result in a blunt instrument that fails to accurately represent the diverse nature of these services.
ii) Please provide the underlying arguments and evidence that support your views.
Response: TechUK proposes regular industry dialogues and check-ins with individual providers, as well as guidance updates to ensure the clarity and relevance of Risk Profiles.
iii) Do you think the information provided on risk factors will help you understand the risks on your service?
Response: TechUK supports the provision of information on risk factors. Continuous industry engagement can further refine and enhance the comprehensiveness of risk factor guidance.
iv) Please provide the underlying arguments and evidence that support your views.
TechUK emphasizes the importance of collaborative efforts to promptly identify and address emerging risk factors. However, the current ambiguity in recognizing these factors raises concerns. This uncertainty may result in companies being unsure of their duties under the bill, leading to potential undercompliance. Moreover, unclear

risk factors could also compel Ofcom to handle cases where companies unintentionally comply with duties beyond their remit. It is crucial to establish a clear framework for identifying and communicating risk factors to ensure targeted regulatory efforts and prevent compliance challenges. TechUK recommends refining the risk identification process collaboratively for clearer industry guidance.
v) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:No

Record keeping and review guidance

Question 10:
i) Do you have any comments on our draft record keeping and review guidance?
techUK supports the need for record keeping and review guidance. Practical considerations should be taken into account, especially for providers of smaller or lower risk in scope services, to ensure compliance without undue burden. Requirements should reflect the individual risk assessment of each service. Aligning with similar international regimes would also be helpful, so smaller in-scope services do not suffer unnecessary burden in data processing the same facts in different ways.
ii) Please provide the underlying arguments and evidence that support your views.
Response: TechUK recommends the development of user-friendly tools and resources to assist companies, particularly providers of smaller in-scope servicesr, in fulfilling record-keeping obligations.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: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?
Flexibility in future assessments is crucial, considering the evolving nature of technology and online services. For example, whether it is not necessary for smaller or very low risk services to have a formal annual compliance review (which Ofcom suggests is the minimum required frequency for compliance reviews at pg 87 in Volume 3)

ii)	Please provide the underlying arguments and evidence that support your views.
TechUK recommends that Ofcom shows flexibility initially as the new framework settles and proposes periodic reviews of this decision thereafter, ensuring alignment with technological advancements and industry developments.	
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?

TechUK acknowledges the flexibility set out in the Online Safety Act, allowing services to either implement the measures contained within the Illegal Content Codes of Practice (the Code), and be deemed compliant with those, or implement alternatives and maintain a written record of how those alternative measures amount to compliance (the comply or explain principle). However, this could lead to an unintended consequence which should be addressed: platforms that choose to implement alternate safety measures, may find themselves penalised through being unable to benefit from the legal safe harbour provided by the more prescriptive elements of the Code.

Ofcom's approach aims to allows services to implement measures that are appropriate for that particular service, which is vital to ensure a dynamic and thriving online environment. However, by having prescriptive requirements, as opposed to principles-based measures that are focused on outcomes, these risk undermining the comply or explain principle. It is difficult to conceptualise what Ofcom would deem as equivalent compliance by reference to very specific requirements. For example:

- 1 **Measure 3E - Tracking evidence of new and increasing illegal harm:** The Code contains a requirement for services to track, monitor and report on different kinds of illegal harm specified in Ofcom's Register of Risks. A number of services are likely to be subject to other similar laws which require them to report on categories of illegal harms. It is not practical for services to have to track, monitor and report against different formulations of illegal harm put forward by regulators. However, it is not clear how platforms can achieve equivalent compliance with this measure in the absence of tracking against those illegal harms specified in Ofcom's Register of Risks.

- 2 **Measure 4I - Use of fuzzy keyword detection for fraud:** The Code requires services to use fuzzy keyword detection in detecting certain fraudulent content. However, many services use sometimes more sophisticated, alternative measures to tackle fraud. Mandating this specific compliance measure could risk disincentivising platforms from investing in more effective measures, due to the risk of losing safe harbour protection by pursuing an alternative approach.

- 3 **Measure 5E(i) - Appropriate action for relevant complaints which are appeals - determination:** The Code requires services to prioritise its review of certain appeals, having regard to specific factors (including the severity of the action taken and whether the action was taken by proactive technology). Each service is likely to have its own approach to resolving appeals which may not fit within this specific framework.

TechUK would welcome further guidance from Ofcom on how services should approach the implementation of alternative measures, noting the prescriptive requirements set out in the Code do not account for the inherent differences between different services regulated under the Online Safety Act. Tailoring strategies based on different risk assessments and other relevant factors including user profiles and functionality is vital to ensure a dynamic and thriving online environment and the proportionate application of regulation.

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?

TechUK supports a risk-based approach which adjusts regulation to the level of risk outlined in the individual risk assessment of each in-scope service, and considers the level of risk to be the main factor determining how a service is regulated under the OSA. However, it is not necessarily true that a large service should be regulated more than a small service where they are both low risk or that large services in this risk category should be regulated more simply because they are deemed able to bear the burden. techUK asks that Ofcom revisit this rationale and align it with the overall approach and the schema presented on p33.

TechUK also proposes that a tiered system should be flexible enough to avoid disproportionate burdens on smaller and innovative in-scope services. While it is reasonable to focus on larger and medium or high-risk services, it is crucial to emphasize that onerous measures should still be applied to smaller services if they are not meeting their duties. For instance, small but extremely harmful sites, should

still be subject to significant measures to ensure compliance and mitigate potential harms. The risk of a service therefore must be the deciding factor here, not size.

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

TechUK emphasizes the need for the level of regulation applicable to each in-scope service to reflect its own risk assessment. Ofcom should avoid over-generalisations and assumptions that may make the day-to-day application of regulation unfair or disproportionate for individual services, particularly smaller services and those provided by SMEs.

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

Response:No

Question 14:

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

A large service has been defined in the consultation as one with 'over 7m monthly users'. However, "service" is not defined in the OSA or in the consultation documents. It remains unclear how providers are to distinguish between features of a service, and separate services, and there should not be a one size fits all approach to what a "service" is defined as and how user numbers are calculated.

Ofcom should also clarify, the utility of using user base in order to establish the size of a service, especially considering that only a regulated part of a service is counted when considering legislation, and what alternative measures have been considered.

Additionally, Ofcom must consider the many definitions of the term 'user', and that this definition is maintained across overlapping regimes and are subject to differing interpretations. Does the definition of 'user' include inactive users as well as active ones? Consideration must also be given to how one counts an individual user. Will 'user' mean separate users or will one individual participating on a platform, for example, buying on a marketplace a handful of times a month, count as separate users?

Clearly, the definition of user will vary from service to service, and the firms running the service ultimately will know best on this. As such, it will be vital for there to be sufficient flexibility for services in their approach to defining users.

Regardless of the threshold, further clarity is also needed on how services that are scaling up will be treated, treated so that the application of additional regulation can be a phased process. The approach needs to be nuanced and flexible enough that they do not impede innovation and scale up of SMEs.

ii)	Please provide the underlying arguments and evidence that support your views.
TechUK suggests collaboration with industry stakeholders to periodically review and adjust definitions based on industry dynamics. We are also keen to understand where there is a review process for the number of users. Given the often rapid change in user levels on services, it will be necessary to make sure that services' obligations are tied to relevant and up to date user numbers, and that these are a real and current measure on how big a service is.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential) No.

Question 15:	
i)	Do you agree with our definition of multi-risk services?
Ofcom has set out 15 harms categories identified in the Risk Assessment Guidance. Services that are assessed as being medium- or high-risk for at least two of the 15 Harms Categories will be subject to additional measures that are aimed at illegal harms more generally, rather than measures targeted at specific risks. However, the harms categories overlap substantially. techUK therefore urges Ofcom to amend the threshold of 'at least two' to 'five' risks. We would also like to ask for the evidence base behind the definition and use of multi-risk services. Further, it will be important to understand whether a multi-risk service with two risks, and a multi-risk service with ten risks would have the same duties imposed on them? Given that case by case assessments may be hard to achieve, it is vital that an arbitrary approach to classification is not taken. At the very least, the threshold for multi-risk services should be adjusted to at least five risks. Additionally, we strongly emphasize the importance of delivering on the Act's intention to be 'targeted' and 'proportionate.' The current definition of multi-risk does not align with these principles, and we propose alterations to refocus on high-risk services. Using the potential engagement of two or more of these overlapping categories to impose heightened general compliance obligations risks miscategorizing a significant number of services as high risk. A more refined definition that ensures specificity and proportionality is crucial to maintain the effectiveness and fairness of the regulatory framework.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: TechUK recommends a dynamic approach to definitions, ensuring they remain relevant and effective in addressing evolving risks.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:No	

Question 16:	
i)	Do you have any comments on the draft Codes of Practice themselves?

TechUK supports Ofcom's intention to create a safe environment for UK users. However the rules must be clear, targeted and proportionate to ensure that businesses can apply them in a reasonable and efficient way, without creating unwanted side effects

The draft codes seem based on a number of assumptions regarding the functionality, level of control and the prevalence of harms in particular categories of in-scope services such that individual services could be regulated in a way that is at odds with their respective risk assessment. This shows some bias arising from Ofcom's very well-developed understanding of some in-scope services but less well-developed understanding of others. For example, the consultation states that "marketplace and listing services are likely to have an increased risk of harm related to terrorism, sexual exploitation of adults, firearms and other weapons and fraud and financial services offences.". Not all in-scope services are the same and should not be treated as such. The drafting and operation of codes must be sufficiently adaptable to different levels of risk and control, intervening only to the extent necessary to address the harm(s) identified in each risk assessment. This should include the ability to disapply individual requirements where the risk or harm is not present, a service does not include the relevant functionality, the user base does not justify the requirement (e.g.: not a service used by children) or the required action is taken by another party in the supply chain.

On balance, the Codes do not allow sufficient flexibility for firms to innovate and use more advanced capabilities to tackle the harms set out. We believe there is a risk that the more prescriptive provisions, e.g. approach to detecting fraudulent content, could unintentionally push platforms to a 'race to the bottom' to comply with the law, rather than take a more sophisticated and effective approach that would not offer the same certainty of compliance. We would recommend that Ofcom frame the Codes more broadly in these instances.

Ofcom further concludes that downstream search services as a whole are in scope of the OSA and this should be revisited. Only services that control which search results appear to users and how they appear were intended to be in scope[1]. Downstream services for whom all their results are provided by an upstream general search engine and have no control whatsoever over the crawling and indexing, are out of scope of the OSA as they are not a "search service" within the definition of Section 226.

Where the drafting of the codes was not preceded by consultation with specific parties, such as downstream search services, Ofcom must undertake this consultation as a matter of urgency and amend draft codes accordingly

Annex 10 guidance on judgment for illegal content applies the same standard of review for non legally binding requests to remove content (e.g. from law enforcement, regulators) with legally enforceable court orders to remove content. For added legal certainty, the guidance would benefit from explaining the factors that platforms should take into account to discharge their freedom of expression obligations when considering non-legally binding requests to remove content (e.g.

requests from law enforcement authorities and regulators). Platforms are not required to perform the same type of freedom of expression analysis where they are legally compelled to remove content by a court order.

We appreciate Ofcom's thorough work in outlining all relevant offences in Annex 10 with extra guidance at volume 5. However, we anticipate that deciding illegality in relation to some offences will be challenging for agents, potentially unnecessarily styming freedom of expression. For example, False Communications is an offence that could apply to many different types of communication on platforms. We would encourage Ofcom guidance to be updated to provide examples of clear False Communications offences, or delaying the application of this non-priority offence until more reported cases can be included in the guidance. We also suggest consolidating the guidance across Annex 10 and Volume 5 to simplify reviews by agents.

[1] *See s703 Online Safety Bill Explanatory Notes*

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

Response:No

Automated content moderation (User to User)

Question 20:

i)	Do you agree with our proposals?

We suggest ACM to be applied only to public communications. While it is referenced at some points in Ofcom's documents, we believe it could be made much clearer in both the Code of Practice and the guidance on public and private communications, that E2EE content is always private and will not be subject to ACM measures.

We reiterate the comments we made in our introductory comments about the need for flexibility for different sizes and types of U2U services. We are concerned that providing prescriptive guidance and technological solutions may not be the best approach, as it takes away the ability for services to assess, and then mitigate, the risks associated with the priority illegal offences in the most suitable way. This is particularly the case for fraud, where risks may manifest in significantly different ways across services, and requires significantly different approaches.

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:	

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'?

techUK seeks confirmation that content shared with a limited group of people should always be considered private, irrespective of the size of that group. Ofcom's guidance currently suggests this is not the case, and so the automated content moderation requirements (to use hash matching, URL detection, and keyword searches) may therefore apply.

We are concerned that the application of a too narrow definition of private communications in Ofcom's draft guidance. The current suggestion that having restricted access controls to file-sharing or storage services does not necessarily make them private, potentially subjecting them to automated content moderation (ACM) requirements, may not align with most people's understanding and expectation of private communications. Even if in theory content is accessible by many people, if those people cannot discover the content without the URL, most people would reasonably judge that to be private.

Therefore, we propose that the guidance should be strengthened to clearly indicate that service providers should, by default, assume that a user taking steps to restrict access to content means that the content should be regarded as communicated privately. In such cases, it should not be subject to scanning or ACM requirements unless the user explicitly indicates an intention to share the content with the wider public.

Additionally, it is crucial to consider the potential replication of the UK's approach in other markets, especially those with less stringent data protection and privacy laws. Therefore, any regulations implemented here should uphold the rightful privacy protections and expectations of UK users. This not only ensures consistency but also safeguards user privacy in a global context.

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

Question 25:

i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
We support Ofcom's approach in limiting "automated content moderation" measures and providing flexibility for services that wish to proactively address broader categories of content, such as all criminal fraud, as opposed to a specific type of fraud offense. This approach recognizes the diverse nature of online services and allows for tailored solutions based on the specific risks associated with different types of content. However, we would encourage Ofcom not to be overly prescriptive in how services address the risk of fraud. To tackle fraud, the use of 'fuzzy keyword matching' could be an effective tool for smaller companies but may not be an effective mechanism for companies that have developed more sophisticated technologies over time to detect this type of content.	
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:	

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.
TechUK supports Ofcom's provisional view to limit the hash matching and URL detection requirements to CSAM. This limitation is crucial, considering the challenges automated technology faces in assessing context for terrorist content. Unlike CSAM, terrorist content often involves complex geopolitical and social issues, making it difficult for automated systems to accurately distinguish between legitimate content and content that may raise concerns. Expanding such measures to include terrorism content could lead to over-blocking, impacting freedom of expression and hindering the dissemination of lawful content. It is imperative to prioritize a nuanced approach that carefully considers the unique challenges posed by different types of illegal content. This approach ensures that online services can effectively combat harmful content without compromising fundamental principles of free expression and open dialogue.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
techUK welcomes Ofcom's efforts in supporting automated moderation. While significant work remains, global multi-stakeholder programs and initiatives have successfully combated key online harms, such as CSE, and we are hopeful that similar, multilateral collaboration can be deployed to combat other types of harmful content. We urge Ofcom to collaborate with industry stakeholders and regulators around the world to create common standards that are globally scalable to protect global users consistently.	
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)

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
There are two main concerns: (i) the provisions are too prescriptive and may not be the best means for individual platforms to meet the underlying harms; (ii) Any provisions around 'Enhanced User Controls' should come alongside Ofcom's broader User Empowerment work in phase 3 of its roadmap. Otherwise there is a risk of misaligned obligations that may be problematic for platforms to understand and implement in a cohesive way.	
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:	

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?
As noted above, techUK recommends that risk is the primary determinant of which rules apply to an in-scope service and that there also be flexibility to adapt codes to individual services depending on its risk assessment, functionality and user base. No service should be regulated for a risk that is not present or a functionality that is not included. Also noted above, techUK recommends that Ofcom creates time and safe space before finalising codes for providers to clarify whether their services are in scope and to consult with providers in more complex supply chains. These changes would better align with the requirements of Schedule 4 and be equitable for providers of all sizes, in particular those that operate differently from the ones Ofcom is most familiar with and on which the codes appear to be modelled.	

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential) No

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

The Illegal Content Judgements Guidance (ICJG)

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
TechUK welcomes the intention behind this question and the recognition that regulation must operate in a way that is equitable for services of all sizes. This consultation is extensive in nature with over 1,700 pages of guidance. While we endorse the consultation objectives, we recommend that Ofcom streamline and simplify its approach to enhance accessibility and reduce barriers to adoption, especially for providers of smaller and lower risk services and SMEs that may face challenges due to limited resources and legal expertise. Ofcom should make resources available for tailored engagement with providers of smaller services and SMEs to enable them to obtain the legal clarity they need, particularly where the services and their risk assessment may not fit neatly in to the framework. Emphasizing proportionality and usability in issuing guidance will contribute to a more effective and widespread implementation of the proposed measures, ensuring that smaller entities can navigate the obligations without undue burden. TechUK looks forward to collaborating with Ofcom to ensure that the guidance is practical and navigable for a diverse range of services, including those with limited legal expertise and resources.	
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:	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response:	

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

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?

TechUK expresses concerns about Ofcom's information gathering powers, particularly the ability to remotely view information demonstrating the real-time operation of a system (Volume 6). This capability raises valid concerns about risks to user privacy and security threats to the functionality of the site. Therefore, techUK requests clarification as to how this right will be used and suggest implementing guardrails to prevent misuse. Addressing these concerns is essential to strike a balance between effective regulatory oversight and protecting user privacy and the functionality of online services.

Additionally, techUK emphasises the sparing and proportionate use of these tools, agreeing with the notion that they should only be deployed when absolutely necessary, without reasonable alternatives. It is crucial to stress that these intense tools should be used sparingly, giving services an opportunity to correct. This approach aligns with the consultative spirit of the regulatory framework, ensuring a fair and judicious application of information gathering tools.

techUK asks that Ofcom follows the lead of other regulators, such as the CMA, which use their information gathering powers in a proportionate and targeted way in recognition of the burden and cost they place on businesses. Requests should be narrowly framed by default. Ofcom should avoid unnecessarily broad requests to 'fish' for information and data not directly related to an individual provider's compliance.

Additionally, techUK would ask that Ofcom commits to sending draft RFI's, which it has stated it may do, so that providers can comment on their scope and request reasonable modifications. techUK believes this is key to making the operation of the UK's online safety regime equitable for providers of services of all sizes and to correct misunderstandings about individual services which operate differently from the ones Ofcom may be most familiar with.

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:	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
The primary focus of Ofcom's resources and effort should be to proactively aid and support providers' compliance with applicable online safety rules and provide actionable guidance to this end. This is the best route to the OSA becoming a stable and predictable legal framework for providers of in-scope services. Enforcement should be a last resort. It has sadly become common in other jurisdictions for enforcement to be considered the singular measure of success of a regime. TechUK recommends that Ofcom explores a broader set of metrics and KPIs to measure its success, such as the balanced scorecard approach used when Ofcom was first created[1]. *[1] See The creation of Ofcom: Wider lessons for public sector mergers of regulatory agencies, https://www.nao.org.uk/wp-content/uploads/2006/07/05061175.pdf*	
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:	