Your response

LinkedIn thanks Ofcom for the opportunity to provide the responses below. We appreciate the reasoned, measured and clearly explained approach Ofcom has taken in preparing the consultation materials. Although they are extensive, the materials are digestible, eliminate ambiguity in various key areas, and provide regulated services a useful set of tools to help frame their compliance solutions. We commend Ofcom for their work in preparing the consultation materials and welcome further engagement on them.

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?
LinkedIn appreciates the thorough approach Ofcom has taken in creating Volume 2. As long as regulated services are able to use Ofcom's Register of Risks as a "starting point" in their assessments and to deviate from it where the Register does not track the actual risk profile of a particular service, it will be a useful resource. We note that, based on the Register of Risks, Ofcom has designed a number of the measures in the Codes of Practice to "target high-risk service types and functionalities." However, although service types and functionalities may tend to correspond with elevated-risk profiles in certain areas, it does not necessarily follow that they should be treated as inherently high-risk. In continuing to develop the Register of Risks and using it to frame the Codes, we encourage Ofcom to consider and acknowledge how certain service functionalities and characteristics (e.g., real identity requirements, professional focus, predominantly adult user-bases) can mitigate risk such that large services or service types generally known to be at high risk for a harm category could be a low risk.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
See above response.	
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.
LinkedIn appreciates Ofcom having set out the *potential* links between risk factors and different kinds of illegal harm. They serve as a useful tool to regulated services in taking a comprehensive approach to assessing risk. However, as noted above, such links should not be treated as inherent. Additionally, such links stem from user behaviour, which evolves (sometimes rapidly and	

sometimes gradually). Accordingly, the Register of Risks will need to evolve to help a service assess risk as they actually manifest on such service.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

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

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
LinkedIn agrees with Ofcom's proposals. The proposed governance and accountability measures set forth in the Codes of Practice (i.e., annual reviews of risk management activities and internal monitoring and assurance functions) serve as an effective means by which regulated services can help manage risk over time.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
The governance and accountability measures currently proposed are appropriate for both large and multi-risk services. If Ofcom proposes any additional measures going forward, it should continue to carefully assess if applying such measures to large services as a whole will be proportionate, targeted and appropriately risk-based, as Ofcom has done in the current consultation materials.	
ii)	Please explain your answer.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 5:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
LinkedIn appreciates the diligent and measured approach Ofcom is taking in gathering evidence of the efficacy, costs and risks associated with imposing such a third part audit requirements on regulated services before imposing any such requirements.	

Baseline standards and success measures for independent third-party audits of online platforms' risk assessment and mitigation efforts have yet to be fully developed and tested. As Very Large Online Platforms and Search Engines undergo their first external audit under Article 37 of the Digital Services Act ("DSA"), we encourage Ofcom to monitor and learn from the successes and shortcoming of that process. Specifically, we recommend Ofcom consider whether application of traditional financial accounting audit processes and frameworks are the appropriate fit. It is, of course, imperative that any third party audit requirement potentially implemented be harmonized with the audit requirement in the Digital Services Act. But it may prove true that the application of more traditional "audit" processes designed to measure enterprise risk (i.e., risk to a business and its owners) is a more appropriate fit in both settings to evaluate services' measures to mitigate online harms associated with illegal content.

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

No.

Question 6:

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

If Ofcom proposes additional measures on point in future guidance, we strongly recommend that such measures focus on company-wide responsibility. Doing so will better ensure the right level of corporate incentives and help avoid unintended behaviours or outcomes.

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

No.

Service's risk assessment

Question 7:

i) Do you agree with our proposals?

Generally, we support Ofcom's proposals on how regulated services can fulfil their duties to assess risk. We welcome the practical guidance provided by Ofcom, including Ofcom's Risk Profiles.

LinkedIn welcomes Ofcom's adoption of a scalable approach that allows regulated services to differentiate based on their size, nature and likely risk profile. In implementing this and recognising the global nature of many services, LinkedIn encourages Ofcom to accept previously completed risk assessments that align to international standards as "suitable and sufficient."

Given that the requirements of the UK's Online Safety Act and online safety regimes in other jurisdictions are not identical, LinkedIn would welcome guidance on the circumstances where Ofcom would consider previously completed risk assessment suitable and sufficient.

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

See above response.

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?
Yes. The four-step risk assessment process and the Risk Profiles strike an appropriate balance between providing clear and practical guidance to services, while simultaneously allowing providers flexibility in light of each service's risk profile.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
The Risk Profiles provide regulated services a clear, thorough and practical resource to help inform how they identify and evaluate potential risks on their service. However, to be effective, the Risk Profiles should enable rather than bind platforms in their approach to identifying risks. LinkedIn commends Ofcom for recognising this and clarifying that the Risk Profiles do not provide a "bespoke analysis" of risk as it exists on a given regulated service.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
See above response.	
iv)	Please provide the underlying arguments and evidence that support your views.
See above response.	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
We generally found the draft record keeping guidance reasonable and appreciate Ofcom establishing clear expectations of what is required while still affording services some flexibility to meet those requirements.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

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?
Overall, the proposed Codes of Practice are very well done. LinkedIn appreciates the thought Ofcom has put into framing them as one streamlined set of Codes to avoid repetition and confusion. We are also encouraged by Ofcom's continued recognition that the Codes should not take a "one-size-fits-all" approach.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
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?
LinkedIn generally agrees, but as noted above, we encourage Ofcom to remain open to the possibility that large services can present lower risks of harm in certain areas such that some requirements may be disproportionate or unreasonable for them to apply.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 14:	
i)	Do you agree with our definition of large services?
Although LinkedIn does not dispute whether it should be classified as a large service for purposes of the proposed Codes, given Ofcom aims to impose reasonable and proportionate obligations on regulated services, we note that the definition's current userbase threshold seems low and likely to result in overinclusion.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
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?
We recommend that Ofcom (1) further refine the definition of "multi-risk" services to prevent it from being overly inclusive or disproportionately burdensome, and (2) continue to carefully assess whether measures should be applied based on the existence of specific risks or a service's status as multi-risk. As currently framed, a service with any minimal evidence of only two types of harms occurring on its service could be treated the same as a service that has ample evidence of the extensive occurrence of all 15 of the illegal harms. Additionally, the current risk classification model overlooks the fact that the 15 illegal harms are not equal in severity. To apply a more risk-based, proportional approach, we recommend that Ofcom revise the definition of multi-risk to only include services with evidence of the material presence of at least four or five illegal harms. Ofcom should also consider incorporating into the "multi-risk" classification process a weighing of additional criteria like service characteristics and the relative severity of the harms at issue.
ii) Please provide the underlying arguments and evidence that support your views.
See above response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Question 16:
i) Do you have any comments on the draft Codes of Practice themselves?
Although the proposed Codes are generally reasonable, clear and digestible, as noted below, there are several aspects of the Codes that require further attention.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Question 17:
i) Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
No response.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?

LinkedIn agrees with Ofcom's proposals. Measures like those proposed by Ofcom have been effective in helping LinkedIn mitigate risk on our platform.
ii) Please provide the underlying arguments and evidence that support your views.
See above response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Automated content moderation (User to User)

Question 20:	
i)	Do you agree with our proposals?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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

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;
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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;
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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

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.
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
No Response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
[✂]	

Terms of service and Publicly Available Statements

Question 29:
i) Do you agree with our proposals?
Generally, we agree with Ofcom's proposals. However, requiring regulated services to publicly describe any proactive technology used to comply with the illegal content safety duties (including the kind of technology, when it is used, and how it works) do not allow sufficient flexibility for regulated services to balance the level of detail with the need to prevent abuse. At a certain level of detail, bad actors are able to learn how to circumvent defences because they know too much about how those defences work.
ii) Please provide the underlying arguments and evidence that support your views.
See above response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

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

Default settings and user support for child users (U2U)

Question 31:
i) Do you agree with our proposals?
No response.
ii) Please provide the underlying arguments and evidence that support your views.
No response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
No response.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Although LinkedIn agrees that services should consider and test the safety implications of changes to their recommender systems, any related obligations to do so under the Codes should be risk proportional. Given services continually make minor changes to their recommender systems, including small A/B tests that are not ultimately deployed, we recommend annual, semi-annual or quarterly assessment of safety metrics of what has actually been deployed.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
No response.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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?
[✂]	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Yes, this entire response is confidential.	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
LinkedIn agrees with Ofcom's proposals. In-product controls like those proposed by Ofcom are important user empowerment tools that help a service's users further shape their experience on the service. Paired with effective content moderation systems, they can help provide users a safer experience on platform.	
ii)	Please provide the underlying arguments and evidence that support your views.
See above response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Regulated services should be allowed flexibility in how they make such controls known to their particular user base. Such an approach would also be consistent with Ofcom's overall proportionate risk-based and targeted approach.	

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

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Yes. If framed properly, voluntary verification systems can be strong user empowerment tools. Specifically, they can provide a service's user base highly valuable authenticity signals to help such users make more informed decisions about what content and individuals they engage with online. For example, LinkedIn is a real-identity online service for professionals to connect and interact with other professionals, learn, hire, and find jobs. Our members look to engage with real people and not with fake accounts, bots, or other inauthentic actors. Accordingly, to complement LinkedIn's robust proactive fake account detection and removal measures, LinkedIn has been rolling out a range of free verification features during the past year, These features allow our members to verify certain information about themselves, like their association with a particular company or educational institution or their identity (using a valid government-issued ID). Once a member has successfully verified information about themselves, a verification badge will appear on the member's profile. The badge will be visible on the platform and other members can click on the badge to find out additional basic details about what information the member has verified and when they did so. Member can manage or delete their verifications at any time by going to their settings.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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)?

Regulated services can use various checks and balances to mitigate the risk that non-violative content will be erroneously actioned as CSAM, including for example a layered use of various detection technologies and human review. Additional examples of these measures and safeguards were recently listed in the European Commission's December 2023 report on the implementation of Regulation (EU) 2021/1232[4].
ii) What are the advantages and disadvantages of the different options, including any potential impact on other users?
See above response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

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?
Regulated services can use various checks and balances to mitigate the risk that non-violative content will be erroneously actioned as CSAM, including for example a layered use of various detection technologies and human review. Additional examples of these measures and safeguards were recently listed in the European Commission's December 2023 report on the implementation of Regulation (EU) 2021/1232[4].
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

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?
Regulated services can use various checks and balances to mitigate the risk that non-violative content will be erroneously actioned as CSAM, including for example a layered use of various detection technologies and human review. Additional examples of these measures and safeguards were recently listed in the European Commission's December 2023 report on the implementation of Regulation (EU) 2021/1232[4].
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
The proposed Codes, as currently drafted, appear to impose a proportionate burden on large services. That said, Ofcom has called out that “all else being equal,” the benefits of a measure will	

be greater when applied to services with larger user bases. While LinkedIn does not dispute that in principle, we have found that is not always the case and that in practice, all else is seldom truly equal even among services with seemingly comparable functionalities. A service's risk profile can be shaped significantly by characteristics other than size — like its purpose, target audience, and whether the service requires users to log in and operate under their real identity. Given these characteristics could render a service with a large user base relatively lower risk[5], as and when Ofcom imposes additional obligations on services via the Codes going forward, we encourage Ofcom to use a more flexible and proportionate risk-based approach.
ii) Please provide the underlying arguments and evidence that support your views.
See above response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

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?
Generally, we agree. As noted in our responses to 47 above, a proportionate, risk-based and targeted approach helps ensure that regulated services' differing risk profiles are taken into account, including the recognition that size alone does not determine risk level.
ii) Please provide the underlying arguments and evidence that support your views.
See above response.
iii) 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 49:
i) Do you agree with our proposals, including the detail of the drafting?
LinkedIn thanks Ofcom for making clear that a regulated service can meet its duty to take action against potentially illegal content by appropriately framing and applying its own terms of service to such content. This is a sensible approach given the global nature of many services, and we appreciate the clarity that the guidance materials provide on this point. That said, LinkedIn notes that a select few of the harms covered by the Online Safety Act (e.g., epilepsy trolling) may be difficult to enforce in practice under terms of service or otherwise, notwithstanding Ofcom's guidance.
ii) What are the underlying arguments and evidence that inform your view?
See above response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Question 50:
i) Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
No response.
ii) Please provide the underlying arguments and evidence that support your views.
No response.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
No.

Question 51:
i) What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
LinkedIn welcomes Ofcom's thorough and thoughtful assessment of information that is likely reasonably available and relevant to illegal content judgments. However, in light of the extensive detail included in the assessment, LinkedIn encourages Ofcom to ensure there is a process in place for regulated services to highlight issues they encounter with the availability of information in practice and areas where further clarity is required.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

No.

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?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
No response.	
ii)	Please provide the underlying arguments and evidence that support your views.
No response.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No.	

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