Your response

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1:	
i)	Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?
Response: No	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Response: The volume of material makes it very difficult to properly assess whether anything of importance is missing. As an organisation our membership being victims or survivors of unlawful violence are subjected to threats/threatening behaviour, abuse and Harassment, which will occur mainly in the use of social media services, and offenders concealing their identity to prevent detection and prosecution. Northern Ireland Troubles related victims are often regarded by some groups as acceptable targets of hate and harassment, with little or no protection, there is nothing contained within these proposals to address this.

There is a lack of awareness by online platforms that posts that may appear innocuous or just "mean", can be the tipping point for the targeted individual, who may have been targeted by many 100's previous posts. The individual should be taken more seriously by platforms when outlining their reasons for reporting abuse. Platforms need to be more aware of the history of Northern Ireland and while we have the Belfast/Good Friday agreement the online hate towards former police officers, security personnel, and their families is still very real. This also includes members of the judiciary during the troubles, their families, and other innocent victims and survivors of proscribed terror organisations.

Many victims and survivors are reluctant to use social media to highlight the injustices they have suffered, as they witness what happens to those who do.

Examples being: A daughter of a member of the Judiciary, who was shot, her sister was killed by a single bullet to the back in the same attack. Her father was shot 6 times, fortunately, he survived, even though he was left critically injured.

The daughter has been subjected to the following abuse on social media.

"Her Dad was a puppet for the brits"

"It's a pity you don't choke"

"They should have put a bullet in your head that day"

"She loves the limelight"

"Her days are numbered"

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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.
Response: Yes, given the recent media attention it is surprising that politics has not been also identified as a motivating factor around online hate crime. Within Northern Ireland supporters of political groups who continue to justify the past and continued use of violence for political ends have used language that amount to hate crimes.	
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?
Response: Yes	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response:	
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?
Response: Yes	
ii)	Please explain your answer.
Response:	
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?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service's risk assessment

Question 7:	
i)	Do you agree with our proposals?
Response: N/A	
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:	

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

Question 8:	
i)	Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response: N/A	
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 9:	
i)	Are the Risk Profiles sufficiently clear?
Response: N/A	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response:	
iv)	Please provide the underlying arguments and evidence that support your views.
Response:	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response: N/A	
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 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: N/A	
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:	

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

Our approach to the Illegal content Codes of Practice

Question 12:	
i)	Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response: The recognition that the this is 'not a one size fits all' is agreeable in the approach to the code of practice, providing the knowledge and security to services. The approach ensures that all services can have an input, providing a clear thorough outline, clear expectations and guidance for services. The approach to illegal online harms spurs the proactiveness needed.	
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?
Response: While agreement is placed in general that onerous measures should be applied to larger services and/or medium or high risk more consistently however, where potential may arise in smaller services to have a deeper knowledge of what onerous measures could be put in place before a risk could escalate may reduce the risk in being more preventative and proactive.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Smaller/lower risk services should have a knowledge of priority offences and the potential for harm or the effects that this may have, for example terrorism. Where terrorists can go undetected or using smaller platforms that are more under the radar in comparison to medium and larger online platform. Where recommendations are made to smaller services there should be a designated person to report. Clear complaints procedures and knowledge of what constitutes illegal harms and the risk factors under the act as outlined in their policies and procedures and mission statements. Difficulties with this in the Northern Ireland context where content may be used to promote and incite hate and terrorism, where this may in other circumstances not arise to illegal the context may be certainly different in the context of Northern Ireland and sectarianism. Within the Northern Ireland context victims and survivor groups may use platforms like social media to communicate and remember those who are victims of terrorism. These are smaller services but could present as high risk within the terrorism category where it can be possible for terrorists to target victims and survivors based on protected characteristics and the ability to indirectly contact users of services.	

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?
Response: While it is agreed that the definition of a large service with an average user base greater than 7 million per month in the UK, approximately equivalent to 10% of the UK population. The 10% of the UK population is a large service seems relatively low in the context where the most onerous measures will have to be implemented and some of the largest services have the ability to cause the most illegal online harm.
ii) Please provide the underlying arguments and evidence that support your views.
Response: While it is agreed that that there is no one size fits all it is noted that some offenders for example, terrorists use larger services in the first instance before moving to smaller groups and therefore the risk of harm for that service will be high. Where smaller services are not subjected to the more onerous control measures because of initial assessed risk and cost. Smaller services should be provided with the same knowledge and awareness. It is noted that users of larger services can move to smaller services and transferring the risk of harm to the smaller service, having previously been classed as a low risk. Smaller groups must be able to mitigate the risk that can change smaller services from potentially low to a medium/high risk.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 15:
i) Do you agree with our definition of multi-risk services?
Response: Yes, we agree with the definition of multi-risk services.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Taking into account at least 2 different kinds of harm from 15 priority illegal harms in order to categorise a service as 'multi-risk' seems sensible, and the additional measures proposed to deal with illegal harms more generally is agreeable.
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?
Response: No
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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?
Response: No
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: Yes, we agree with the content moderation (User to User) proposals
ii) Please provide the underlying arguments and evidence that support your views.
Response: When services are deciding which potentially harmful content should be prioritised for review, they need to consider that the NI context is very individual and terrorism and hate offences may not be easily detected by automated tools. A bespoke approach to content moderation for Northern Ireland based potential harms is essential as content in videos and written words which have the potential to go viral and cause the most online harm may not be obvious to those not familiar with the context of terrorism and hate in Northern Ireland. Human review of potentially harmful content should be prioritised for this jurisdiction but in implementing this, specific training should be given to make moderators aware of examples of

terrorism and hate applicable to the Northern Ireland context. Victims and survivors of the Northern Ireland 'Troubles' are being targeted by accounts online who wish to minimise their trauma and loss and in reporting these hateful messages, victims and survivors have not received support from the social media conglomerates as there is no understanding of the context in which the glorification of terrorism messages have been written. The automated moderation should also be tailored in such a way that it can identify the specific language used in Northern Ireland to harm, insult and terrorise innocent victims and survivors of the 'Troubles'.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
Response: No	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: These measures will deindex or downrank material without removing it, those organisations / persons who control websites which mock, demean, or harass victims will be widely known among their constituency / users / observers, although minimising it's ranking on large search engines it does not seek to specifically target the unlawful nature of such content, specifically with regard to the Terrorism Act 2000. The proposals have been written in a fashion that seeks to deal with harmful rather than illegal / terrorist propaganda, thus ensuring that the element of harm for the victim remains as no attempt has been made to criminalise this material. Where material is identified as illegal, the power remains with the search engine to keep the website in place, listing it further down the search if the majority of material on the website is not criminal. The control for downranking and deindexing remains within the search engine and is moderated at their discretion.	
iii)	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?
Response: N/A	
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'?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response: N/A	
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: 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;
Response: N/A	
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: 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;;
Response: N/A	
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: no	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response: N/A	

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.
Response: N/A	
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:	

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Currently, there is little evidence to reflect what systems are in place by small, medium, and large organisations. This could give concern to a lack of proactive participation in attempting to mitigate the illegal harms of terrorism and actions by proscribed organisations. Larger companies use several layers of operating systems to monitor for illegal content, however, research suggests that these are mostly automated. There needs to be an indication of how robust or specialist the filtration systems are. Smaller companies are more likely to use human resources to manually search. This can give way to subjective bias based on personal beliefs or knowledge. Risk assessments can be a useful tool in the aid to triage queries however it should not be used as a stand-alone tool.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: By placing an onus on the organisations to have a timeline in which to investigate and respond to complaints, there should be protection given to the complainant that their concerns will be addressed and responded to. Providing reassurance and accountability that complaints are heard	

should bring confidence to the security and safety of an organisations so that if further illegal harm arises then complainants will come forward. However, this timeline should be realistic instead of dismissing a complaint simply because the timeframe wouldn't be achieved, and a corporate "target" failure avoided which in turn keeps stat numbers low. This is a provision already in place by X (formerly twitter) as an acknowledgment is received and updates are provided through the user's twitter platform notifications. If the complaint has not been responded to in and more time is needed to review the content, then a notification is sent to the user to update them on the details. This is a good practice to keep the complainant informed and provides validation that they have not gone unheard. The notifications, however, are automated and have a clinical tone, especially if there has been a series of complaints made which can make the process feel impersonal. A proposal to readdress the complaint with free text options to outline further the circumstances surrounding a complaint may be an option as human resources can take a deeper look at a complaint rather than automated systems. There is an appeal to the human side of a situation that AI technology does not understand.

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

Response: No

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response: N/A	
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 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response: N/A	
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:	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response: N/A	
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 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response: N/A	
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 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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

Question 36:	
i)	Are you aware of any other design parameters and choices that are proven to improve user safety?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enhanced user control (U2U)

Question 37:
i) Do you agree with our proposals?
Response:
ii) Please provide the underlying arguments and evidence that support your views.
Response: Response: Again, an oversight of processes as opposed to individual content, the large social accounts Twitter, Facebook etc, will retain their models, ultimately ran from the US with Northern Ireland bases law enforcement / civil claims needing to make applications to the US authorities for any information relating to those behind the offending account, this does not go far enough to tackle the specific online harm which relates to terrorism and harm of victims in Northern Ireland. Specifically – There would need to be more information on how civil society can participate in this, Victims groups in Northern Ireland would be uniquely qualified to highlight / flag material which they deem as inappropriate / terrorist related.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 38:
i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response:
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

Question 39:
i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response: Voluntary verification schemes have been in use on some platforms for some time (such as X formerly known as Twitter) but the user should always easily be able to ascertain for what reason the account has become verified. Verification schemes can involve meeting certain criteria and give an account a certain status online ie verified notable figures in society. If the scheme simply involves a subscription type model then this does not automatically create safety for the receiver of online hate from that account but does mean that the account is traceable back to a bank account and can be more easily identified and accessed by authorities if needed to investigate possible criminal charges if said account has posted or targeted hate/terrorism content. The risk of paid verification schemes being rolled out is that this can create an illusion of safety to other users but in reality does not stop the verified account from posting online harmful content.

A voluntary verification scheme should be available to all users on all platforms which means that the identify of every account can be available to authorities if ever needed but also available to the services themselves so that they can track patterns of online harm being posted by one user having multiple accounts.
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.

User access to services (U2U)

Question 40:
i) Do you agree with our proposals?
Response: Yes but we think that the proposals could go further.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Services should remove a user account from the service if they have reasonable grounds to infer it is operated by or on behalf of a terrorist group or organisation proscribed by the UK Government (a 'proscribed organisation') – this measure is agreeable but services must take measures to ensure it is not easy for the originators of that account to simply set up another account and perpetuate the offence for which they have been removed. Email address / IP address/ Bank details should all be flagged so as to negate the risk of a harmful use simply returning to the service under a new account. Verifying user identity at the point of setting up an account would mitigate against this risk. We believe preventing access to services once illegal harm online has taken place is the best way of eradicating online harm.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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)?
Response: N/A
ii) What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:

Question 42:

i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

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

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response: N/A	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response: N/A	
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:	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response: N/A	
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 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response: N/A	
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 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: Yes	

ii)	Please provide the underlying arguments and evidence that support your views.
Response: A broad question that needs further fleshing out however there is a deeper accountability for large organisations to take the safety and security of their users into account. They represent a larger cohort of users and therefore there is a larger responsibility on their shoulders to offer protection on a wider scale. This is because there is more room for issues to arise, especially when dedicated oversight to every post, comment or communication cannot be monitored 24/7. An efficient and proactive monitoring system will help to deter these types of illegal harms happening on their platforms but coupled with a robust complaints procedure, there will be a benchmark set that it has a no tolerance attitude towards harmful and illegal activity. With consideration being given to large services that not unduly impacted by being the test subject to the new measures, by beginning with low risk measures they can plan a strategy for how they implement the initial steps before taking on more high risk measures.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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?
Response: N/A	
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:	

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

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response: N/A	
ii)	What are the underlying arguments and evidence that inform your view?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response: N/A	
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: N/A	
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?
Response: N/A	
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?
Response: N/A	
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:	

Annex 13: Impact Assessments

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