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: Our company wishes to make specific observations about the appropriate use of E2EE in a health tech context. We all expect absolute confidentiality when engaging in a consultation with a clinician. E2EE can provide appropriately highly assured controls of that confidentiality (noting nothing is digitally cybersecurity perfect, much as someone could listen at your consultants door) – without which other security methods ALWAYS risk confidentiality breach due to administration rights access and hacker privilege escalation techniques. It is also worth noting the NHS already mandates that all audio visual tools are E2EE when used in consultation. We argue this decision should extend to other information exchanges between clinician and patient that directly relate to the content of the consultation – otherwise they undermine confidentiality (e.g. when shared via email or SMS etc). Consulting with NICE they have agreed we have highlighted a “potential gap in our <NHS> pathways”.

Our key point to make is wrt to this section of your document highlighting E2EE as a concern. What this misses is that when one of those participants is a TRUSTED individual (a registered clinician duly evidenced as trained) then the risks the rest of your document refer to in this respect really don’t hold serious concern, in the same way as confidentiality trumps informational content sharing in a face to face consultation, the same should hold true if that consultation is facilitated digitally.

We believe this section should make exception for clear use cases where one of the participants is assessably TRUSTWORTHY when using E2EE as that effectively separates your broad statements from ones where E2EE is not only better than other cybersecurity methods, but demonstrably already in use in important to sustain.

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

Response: A more nuanced understanding of E2EE and its benefits is critically needed along in order to appropriately position the risk and benefit of E2EE and relate to identity of at least one Trusted party in the communication.

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: We believe the tone and approach to E2EE is overly aggressive and insufficiently nuanced. It misses the (often more significant) risks associated with using other encryption methods between communicating entities. Specifically:

1. Using a 3rd party key provider (e.g. multiparty SSL/TLS) puts content TRUST into a 3rd party and creates a lack of accountability and assessability when such key dissemination methods are compromised
2. Any other crypto key management system ensures that the facilitating entity (e.g. Facebook, Google etc) has ultimately always got access to the content of communication.

Both of the above lead to regular compromises communications across the internet as everyday reports from all cyber hack orgs demonstrates. Healthcare consultations MUST be TRUSTED as CONFIDENTIAL if the UK is to be able to leverage the Internet as an asset in healthcare delivery.

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: no.

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

Response: The evidence continues to pretend that E2EE can exist alongside 'appropriate measures' whilst holding a specific person in a company accountable for "illegal content duties" which are clearly not executable when using E2EE. In effect this is removal of E2EE from service provisions due to holding a specific person accountable to an as yet undefined set of standards.

The key issue in this is in innovative investment support. For example our company received a UK Government Innovation Grant to specifically innovate, using E2EE, a method by which consultations can be supported and extended into managed self-care support whilst sustaining confidentiality assurance for patients. While the tech is complete and demonstrable, early prospective customers are raising questions as to whether the confidentiality innovation is sustainable in the face of the Online Safety Bill in the medium to Long Term (once it extends beyond the large scale social media types of businesses initially targeted). Worse, Angel investors, are also pulling back from any form of business innovation with a risk element, and the Online Safety bill is now a significant risk for investors given the unknown real situation of enforcement for smaller businesses in the medium term, and the assured consequences once the business gets to a large size, despite the previous point that online consultations in healthcare clearly need a standard of protection equivalent to or as close as possible to, a private conversation face to face.

Governments like Australia have been able to provide an assurance framework with specific guidance on patient safety when E2EE is used - https://www.esafety.gov.au/industry/tech-trends-and-challenges/end-end-encryption it is CRITICAL that OFCOM brings forward similar guidance ASAP if they agree that the clinician-patient consultation process deserves the highest standard of encryption and confidentiality assurance E2EE can provide.

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: No.

ii) Please explain your answer.

Response: There is insufficient clarity on when/how smaller organizations will need governance, when this will occur or to what standards. This has a chilling effect on certain types of innovation, like our own, and on the investment community who are as unsure as the business entities themselves as to what impacts there will be in the future, including the effective banning of the functional tech underpinning the innovation, like E2EE.

Clearly not all questions can be answered before they are addressed. However an insightful perspective on the peer to peer nature of E2EE and what this means when one of the peers is a Trusted person in the context of technology use is needed. OFCOM could make statements in this regard that would open this pathway up for sustained innovation, investment and E2EE adoption with a clear limitation of why and how that exclusion can/should exist.

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:

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: One has to wonder whether any serious investigation of the safety critical systems market has been reviewed in this regard? Systems such as aircraft control systems, nuclear power plant control systems etc. These markets are often referred to as OT (Operational technologies) as opposed to IT (Information technology). These are sectors this author has worked in historically. They set standards for software safety assurance. It is just a consideration to ask companies building such safety critical OT systems how they motivated the developers of these systems to drive safe outcomes? Note in these systems there are measurable objectives for safety – as highlighted in OFCOMs report such measures do not exist yet in the primary sectors of concern. However maybe those developers were additionally motivated by methods other than just measurement versus industry accepted safety standards.

One area that may help to understand the challenge is to understand the mapping between Trustworthy people and Trust points in cyber security implementations. That mapping can be done relatively straightforwardly by understanding access rights and controls in the context of the accessible data types, to resolve to a clear accountability function and responsibility associated with such access rights as a Trusted person mapped to a secure digital trust point.
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?
Response: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: Very high level guidance that follows basic resilience and safety assessment governance followed in many other sectors.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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?
Response: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: As a product manager of 25+ years experience including in safety critical software development, these are basic first steps in the right dirction.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response: Bit high level, many assumptions of how to apply to real world use cases are the only way to validate them. Overall a good start point.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response: Yes	
iv)	Please provide the underlying arguments and evidence that support your views.
Response: 25+ years software systems development experience including in safety critical systems.	
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?
Response: No	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: The software development needs to take user safety into account properly and the governance requirements herein are a minimal start point.	
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?
Response: The “large” definition is clear to define the application of controls. What seems very unclear is what is a risk in multi-factor risk. For example if EE2E is used on gets the broad impression that high risk is assumed U2U. However as previously highlighted, it is not clear if E2EE used where one peer in the communication is Trusted, whether this reduces risk to a level where it no longer falls into the multi-risk category driven by E2EE use in the context of the Online safety’s Bill approach to the tech as a risk creation factor. Obviously guidance on what a Trusted person is and how to manage them and how to provide safety features for when a trusted entity becomes untrustworthy from the PoV of the other peer participants.	
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: yes on Large, unclear on High Risk assessment and what fits this category.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: Reading the guide the lack of a Trusted participant in E2EE use as a risk mitigator is not understood or communicated.	
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: Yes	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: N/A	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:NO

Question 15:
i) Do you agree with our definition of multi-risk services?
Response: No
ii) Please provide the underlying arguments and evidence that support your views.
Response: The definition of what is a Risk in the context of certain tech functionality is unclear. It feels like the law makes this unclear and hence enforcement is similarly unclear.
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:N/A

Content moderation (User to User)

Question 18:
i) Do you agree with our proposals?
Response: To some extent
ii) Please provide the underlying arguments and evidence that support your views.
Response: It is not mandated that the content is visible to the service provider, only that they are capable of taking it down should they be made aware of it. It is worth noting that a user in an E2EE system can identify offending content to the service provider and that can be taken down without the service provider ever seeing the content. This only works if users are considered trustworthy enough to request content removal and for offending content to be flagged. Nothing in E2EE stops a user taking such content and sharing it with OFCOM or, as in our case, a Trusted service provider who can be requested to act appropriately against the offending content creator.

However, in our generalisable use case, users expect confidentiality in their information sharing. So no pre-content assessment can or should be done otherwise it breaks confidentiality in healthcare. So the guidance is little unclear, on the on hand stating clearly responsibility is solely to take down content – but then implying the method necessitates pre-view before posting – in healthcare this may not make sense and should not occur – however alert/response systems from patients and/or clinicians (after due ethical consideration) should be enabled.

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

Automated content moderation (User to User)

Question 20:
i) Do you agree with our proposals?
Response: No
ii) Please provide the underlying arguments and evidence that support your views.
Response: Exemptions are needed versus automated moderation when, as discussed previously, when user confidentiality trumps risk of content sharing such as in healthcare, and where, in effect, a human moderator exists on every communication because one of the parties is a Trusted person (clinician).
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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'?
Response: No
ii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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;

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

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:N/A
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: N/A
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:n/a
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: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.
Response: Such content should remain confidential in a clinician-patient consultation and or information exchange. Ethic clinical guidance determines when/if such content should be shared with appropriate services.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Fact of existing practise that should not be altered by this legislation, yet no exemption has been explicitly rcognised.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Automated content moderation (Search)

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

User reporting and complaints (U2U and search)

Question 28:
i) Do you agree with our proposals?
Response: Yes noting that in an E2EE healthcare consultation system the service provider is NOT the organisation that can be held accountable for responding to such issues as they do not have access to the content. However such a platform provider must create Service Level Agreements and service facilities to ensure the Trusted parties at the service organisation using the platform can comply to this service requirement.
ii) Please provide the underlying arguments and evidence that support your views.
Response: n/a
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Terms of service and Publicly Available Statements

Question 29:
i) Do you agree with our proposals?
Response: Yes
ii) Please provide the underlying arguments and evidence that support your views.
Response: n/a
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

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

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: n/a
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:no

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:no	

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: n/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:no	

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: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?
Response: n/a	

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

Response:no

Enhanced user control (U2U)

Question 37:

i) Do you agree with our proposals?

Response: In general yes – however there is a bias towards guidance towards an assumption of social media like services and the guidance fails to be wide enough or clear enough for other services to have a confident interpretation for their own business and product implementation.

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

Response: N/a

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

Response: No

Question 38:

i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?

Response: No not as currently defined in guidance.

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

Response: No

Question 39:

i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?

Response: Yes – especially in healthcare. For example it is VERY unclear to patients what type of qualification is appropriate to assess that a mental health practitioner is appropriately of sufficiently qualified to be a TRUSTED remote service provider. This is true not only in general clinical qualification, but additionally, training to cover additional risks that should be managed when delivering care remotely. It is also similarly hard across other health professions and while the NHS has an accreditation control system, the private sector lacks any central repository to validate that a claim of identity relating to qualifications is true and trustworthy. Hence many health service brokers provide their own assessments and are not audited to have done so appropriately in all cases, leaving it to the patient to determine if the claims of trust and trustworthiness of the clinician are appropriately voluntarily validated through such 3rd parties. OFCOM needs to address this factor as the next big issue is going to be abuse via 'trusted' clinicians no matter what underlying delivery technique is used.

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

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: no	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:n/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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?
Response: unknown, we are unqualified to suggest.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: 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?
Response: A bit lik two or multi-factor authentication, ideally more than one assessment service should be used, ideally 3 from separate providers, with a voting system.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

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:n/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: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?
Response: No. The issue is not whether the measures themselves are cumulatively proportionate, but whether the impact of them are appropriate. As previously highlighted there is a chilling effect on secure systems innovation and early stage investor confidence of the cumulative complexity of these enforcements, lack of wide enough exemptions for specific sector use cases, and ultimately risk to businesses generally to be based and develop in the UK. Ther is already a significant drain to the US and this lack of clarity will drive start ups to more readily consider going to the US first.	
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 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: potentially, but needs nuance as stated previously around the idea of trusted users in the U2U communications.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:n/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:no

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: n/a	
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: some are, but more work is needed to clarify application across wider sectors instead of being blinkered by the social media problem and treating all entities in the market as some sub-form of their problem. They are not, they are often distinctly different and the enforcement regime fails to recognise this.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:n/a	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:No	

Volume 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:	
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:	
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?
Response: It is unfortunately problematic, that OFCOM seeks answers to this consultation via email which is notoriously not confidential, yet asks in every section whether the answer should be kept confidential – the sending mechanism is not confidential! Otherwise ofcom sems to be starting with a self constrained approach which may in fact undermine its own efforts to change attitudes in the business sector from the big tech orgs.
ii) Please provide the underlying arguments and evidence that support your views.
Response: n/a
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:no

Enforcement powers

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

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:no	