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?
Threats, Abuse and Harassment, including Hate is very broad and would impact on free speech, you don't solve hate by suppressing it, and of itself is not negative. You can hate something because of its negative effects on women, culture, rights etc	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
The compulsory registration of all users of the internet with passport or other ID on multiple platforms (Google, Windows, Apple, FB, Twitter etc) is necessary for age verification and banding and tracking and more dangerous that the other harms you are seeking to mitigate. It is clearly implied thoughout that EVERY user on EVERY platform will be identified and tracked. Already, Google and Microsoft are demanding ID upload for verification due to "child safety" due to the OSB. Google pays Apple $20 Billion per year to use Google as the search engine in Safari, once registration is complete, forced by the OSA, every physical movement (phone), search, Word document is available for data harvesting for all users. For users, and particularly minors, this means that each and every foolish action/view will be available to worldwide security services and blackmailers, and tracked in the entire world as databases are replicated worldwide and will be stored where the provider chooses in jurisdictions where little if any regulation applies. Once the child (or adult) uploads their passport details, they will be tracked physically, which site the visited, what friends they have etc. Obviously to finance the billions involved in the foolishness, I.T .companies now can (as they obliged to collect passport details) and must, to pay the costs of this insanity, charge users fees for site usage. The comments that age assurance technology may be used is also nonsense, no company is going to spend millions connecting to some sort of anonymous verification service when they can snatch and sell your details via Gmail login/Windows login etc. I am very concerned and the complete lack of basic understanding OFCOM seems to have of the economics of the internet and the drivers for data collection. The OSA is an act of madness and utterly irresponsible, most internet access traditionally has been anonymous, but the OSA will enforce tracking via Google and other systems. Most of this data will be stored in multiple worldwide locations accessible by the security services/blackmailers/fraudsters of the respective countries. This is not Online Safety, it is the exact opposite and is deeply dangerous particularly to minors, and will have major impacts on national security. is not entirely clear this will be acceptable to other nations that may object to the wholesale tracking of its citizens through UK mandated ID verification. It also means any internet usage by refugees or dissident will be instantly tracked worldwide.	

Above is the main cause of online harm which will have major impacts on democracy, freedom, the economy and national security not the threats you are failing to address. See also: https://stoptheonlinesafetybill.wordpress.com
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.
As per Q1 ii.
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?
No. It is not clear how you will assign liability for a platform hosting a service (Say a blogging site), the service (Individual or company site with U2U services) or a commentator or content, or apply it worldwide. A code of practice may work for a house windows installer, but not for I.T. It is foolish to attempt it. Simply indicate what is illegal etc and prosecute were necessary. You do not have the right to impose UK law on overseas entities especially if those countries still uphold freedom, privacy, and democratic values. This runs contrary to other nations' law on freedom and privacy – as data and solutions are mostly stored overseas, this is in effect colonialism and imperialism. Who do you think you are?	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Fail to understand how to identify your target – a blogger? A forum moderator? The platform on which it is on? A comment made? It is not realistic to expect a company based in China, India or the U.S. to submit to this nonsense or how it would be enforced. How many millions of companies does Ofcom intend to contact every week to update their information?	
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?
No. It is completely unrealistic to expect a worldwide company based overseas, or very small companies to spend 10s of £10k on state specific measures that are largely pointless. It will isolate the UK to the point that either the UK is made to look very foolish, or services will be withdrawn. Innovation and creativity will cease – no small startup can risk the huge fines and corporate governance required – most of the expensive measures apply to very small sites. We need only look at the damage done to charitable institutions by compulsory risk assessments etc – many closed and activities curtailed, far more harm than good.	
ii)	Please explain your answer.

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?
Not even sure which entity you wish to audit. The main calculation seems to be to provide massive contracts to large Service Providers ultimately paid for by the taxpayer. I am not sure how the UK Gov. believes it will audit, or even identify the millions of sites worldwide. There is also a danger that selection will be politically motivated, eg: A Feminist organisation may be targeting for questioning identity (I don't take a position on this, but it is a matter of free speech) A U.S. company will not want British auditors conducting audits on their systems, accessing confidential information.
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?
I.T. companies are not the Civil Service, they are normally composed of 10s or 100s of different companies providing different services in a mesh, it is really unclear who you are targeting or why, attempting to manage I.T. as if it were a local plumbing company. Very large IT companies have 100ks of employees with complex lines of responsibility. It is not the job or within the remit of the UK government to tell private companies overseas how to run their businesses, or impose measures not imposed, or contrary to, other sovereign nations. The arrogance is breathtaking.
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?
Not for OFCOM to demand a helf' and safety review, too prescriptive

ii)	Please provide the underlying arguments and evidence that support your views.
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?
As Q7.	
ii)	Please provide the underlying arguments and evidence that support your views.
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
As per Q7	
ii)	Please provide the underlying arguments and evidence that support your views.
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
iv)	Please provide the underlying arguments and evidence that support your views.
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?
Ridiculous. Content comes and goes every second on web sites.	
ii)	Please provide the underlying arguments and evidence that support your views.
Common sense and decades of I.T. experience	
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. The basic premise here is that potentially exempt services must spend vast sums of money when in fact they should be exempt. This is in effect fining someone for something they haven't done. The utter contempt for the businesses' money and survival mandating they are liable to do something they may not need to - shocking. It was a maxim of English law of innocence until proven guilty and the all is legal, unless illegal – this contravenes these principles.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
Most of it is technical nonsense with a few buzzwords thrown in and are either already ineffective or partial at best, it is very hard to understand how a government entity thinks it has the expertise to prescribe to companies how to screen their platforms or how smaller businesses or people can be expected to comply - money wasting nonsense. Too prescriptive trying to tell experts how to do their jobs, just set goals and fines where required.	
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?
As they are in the main pointless or unenforceable better not at all.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
It is not possible to agree with something that is completely illogical. 7 million users? Accesses? Including/excluding access by unregistered users with links? Active or inactive, ones that logged in the UK and also, say India? Federated users from other services? It is total nonsense.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
No, it is a complete waste of time to develop some sort of taxonomy of IT services, they are transient, ephemeral and constantly mutate, a bureaucratic, money wasting mind game.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As above, it would be better to simply stick to existing offences and prosecute when required.	
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?
As an I.T. professional with 30+ experience these costs and time estimates are ridiculously low unless, as in the case of large companies, they have some of this already. This will break most companies, particularly small ones, involving very major engineering and endless updates. I am perplexed as to how a Gov Dept. could possibly think it could calculate this. Suggestion: Stick to the day job.	
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?
No, It is very hard to understand how a UK only based internet is going to be economic or run. It seems the intent is that a large provider such as Google must censor each and every page for the UK users only but not for any other country, nonsense. There is no other practical way of adhering to UK regulations unless, as appears to be the case, the UK intends to dictate to the rest of the world want content it can/not host. Please engage with I.T. literate experts before proposing this nonsense.	
ii)	Please provide the underlying arguments and evidence that support your views.

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 It is very hard to understand how a UK only based internet is going to be economic or run. It seems the intent is that a large provider such as Google must censor each and every page for the UK but not for any other country, nonsense.	
ii)	Please provide the underlying arguments and evidence that support your views.
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 As per response to Q18 and Q19.	
ii)	Please provide the underlying arguments and evidence that support your views.
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	
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;
An image can be changed by altering one pixel so except for some limited instances where an inflight image can be removed, it is largely pointless. How does the UK government intend to force an overseas company to control this when only the image may only be visible in the UK?	

ii)	Please provide the underlying arguments and evidence that support your views.
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;
As per Q22	
ii)	Please provide the underlying arguments and evidence that support your views.
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;;
All but the largest companies will need to shut down due to high costs, this is a bonanza for large companies who will be in a monopoly position driving all innovators out of business, which I suspect has much to do with the driver for the OSA.	
ii)	Please provide the underlying arguments and evidence that support your views.
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;
Leave fraud detection to people who are qualified to do it. It is not for the any government to mandate how this happens, only establish and offence for allowing it. Too prescriptive and again, a UK only Internet is not going to work. Such a waste of time and money, the money wasted on this bureaucratic, unimplementable, and unenforceable mess of the OSB could have been used to actually tackle fraud.	
ii)	Please provide the underlying arguments and evidence that support your views.

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.
As above	
ii)	Please provide the underlying arguments and evidence that support your views.
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. In the short term, content moderation appears to protect people from offence, hate etc, but I remain of the view it is better to allow this so it can be challenged. For example, if a crank states the holocaust didn't happen, then, if this is public, it can be challenged and refuted with irrefutable evidence, hidden, a/ the crank continues to believe nonsense b/ they acquire a mystique of knowing a secret nobody else does. Except in very extreme cases it is better to challenge openly rather than, unknown the users, deprecate content the UK government doesn't approve of. If this is done, then THAT must be transparent and not as currently the case simply put out of sight as if these issues don't exist.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As per other responses. This can lead to denouncements, name calling and virtue signalling without due recourse. As very little of this is in UK jurisdiction is is unclear how it would work.	
ii)	Please provide the underlying arguments and evidence that support your views.
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
As earlier, if the service provider can dictate what content it will allow the danger is only left, or right, wing views are tolerated, a situation OFCOM is clearly happy with.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
Stick to the day job, not for the government to prescribe each and every design and danger.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As per Q1 ii. The issue here is that companies will as Daniel Goldhagen explains in "*Hitler's Willing Executioners*" Perfectly ordinary bureaucrats will "*work towards the Führer*" and basically brand anybody that even attempts to talk to a child a paedophile, meaning nobody will dare even help a child with homework.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
In a liberal democracy the responsibility is on the individual to manage their own settings, not for the nanny state to dictate each and every possible threat. A small government campaign is not a bad thing, but you don't need a Online Safety Bill for that.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
The should be clearly warned of the threats they face of blackmail, lifelong tracking of each and every movement imposed by these proposals.	
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?
How will worldwide companies run a worldwide internet and an UK based one with its own requirements – Sorry the British empire is long gone, get over it.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
What does a regulator have to do with it?	
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?
Online anonymity or at least obscuring of personal details such as passports, addresses etc. The proposals will mandate ID uploads which in turn will be linked to consent for "marketing" to "partners" so is very, very dangerous, the OSA will INCREASE Online Harms not reduce them. The underlying assumption here is that users must be identified, minors or not.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
What on earth does this have to do with the UK Government? Most offer this anyway, and if you don't like it, leave. Commercial forces will resolve this, ie a Twitter storm about certain content or features will resolve this, it doesn't need totalitarian regulation.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As per Q37	
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?
As per Q37	
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?
As Q37	
ii)	Please provide the underlying arguments and evidence that support your views.
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)?
As per Q1. Ii. EVERYONE will need to provide their ID to ALL providers so this can be effected, total loss of privacy, and will mean one user unfairly blocked would be blocked from all services as they would be known to all providers via their passport ID.	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
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?
Ref Q1 ii.	
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?
Just let the industry sort it out and prosecute violations, it is the duty of the government to enforce the law, not prescribe how that is to be achieved, that is the fundemental mistake of OFCOM and the OSA.	
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?
Too prescriptive, stick to the day job.	
ii)	Please provide the underlying arguments and evidence that support your views.
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

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 – This will cost the economy billions to implement, drive small businesses out of business, close down I.T. innovation and operation in the UK, it is totally impractical and unnecessary. It is in effect a return to Russian/totalitarian surveillance.	
ii)	Please provide the underlying arguments and evidence that support your views.
Most small businesses or bloggers simply don't have the resources to implement the massive and unnecessary bureaucracy involved.	
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?
As per Q45.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As per Q45	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
NO Stick to enforcing the law not prescribing how it should be achieved by Russian style regulation and state surveillance.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
The underlying assumption is that if the service provider censors legitimate content such as discussions around trans, immigration or other topics that is good as it goes further than OFCOMs censorship, no attempt is made in any of this to defend democratic rights to self expression or have legitimate debates around contentious issues. The anti-democratic, censorship mindset of OFCOM, and the whole spirit of the OSA which can be summarised as totalitarian command and control is very, very clear.	
ii)	What are the underlying arguments and evidence that inform your view?
Adolph Hitler, Stalin, Mao or anyone else you care to name.	
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?
As above.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As earlier, T&S allow companies to overly restrict content or working towards the Führer as OFCOM will be waiting to issue a fine.	
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?
The government cannot be trusted with this power, it is too prone to abuse and targeting of enemies of the state.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
As stated in earlier responses, unimplementable, prescriptive, and fundamentally misjudged.	
ii)	Please provide the underlying arguments and evidence that support your views.
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?
Not worthy of an answer, what an utter and total waste of taxpayers' time and money.	
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.
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
No	