

Your response

Question	Your response
<p>Question 1: Do you have any comments on Section 3 of the draft guidance on harmful material and related definitions?</p>	<p>3.5 - 3.9 Aligning the definitions of Restricted Materials with those already applied by the BBFC provides a clear signal services of which content is likely to fall into the Restricted Material category.</p> <p>3.16 states that “material which might impair the physical, mental or moral development of under-18s is likely to evolve over time” – It would aid understanding if an example can be added to illustrate this statement. The test for harm should be as straightforward as possible – we are concerned this statement gives room for argument over whether, for example, content which Ofcom or a court has ruled harmful yesterday is no longer harmful today.</p> <p>3.16 It goes on to suggest “VSP providers should ensure they remain informed about changing attitudes” – placing on services a duty to monitor the moral compass of society is an onerous responsibility It would again add clarity if any example can be given of how changing attitudes would affect the level of impairment experienced by a child.</p> <p>It may be less confusing to remove this paragraph, and in practice, for Ofcom to produce guidance to assist providers in understanding what is and is not likely to impair the development of children, which will build on examples from enforcement action and case law. Then, in a more traditional manner, should a provider think attitudes have changed, it can test this via Ofcom and ultimately the courts. With that guidance should be advice on the level of protection mechanisms that is appropriate.</p>
<p>Question 2: Do you have any comments on the draft guidance about measures which relate to terms and conditions, including how they can be implemented?</p>	<p>4,18 “Terms and conditions should” – is this not a “must” or at least “must” should be inserted before “ “specify that videos” to be consistent with what has been stated already above?</p> <p>4.51 repeats the point made in 3.16 but alters the logic to say “material which might impair the physical, mental or moral development of under-18s is likely to evolve over time” – so ‘material’ rather than ‘attitudes’ – this inconsistency does not help understanding of what is expected of services seeking to comply. The rate at which children mature is not uniform across individuals but its average is relatively constant, meaning what would impair the development of the average child of a particular age yesterday will still impair them tomorrow to the same degree – society’s attitudes have no direct affect on this.</p> <p>Achieving a common understanding of what is expected of services to deliver consistent regulation and a level playing field could be made more difficult by these somewhat confusing provisions in the regulations.</p>
<p>Question 3: Regarding terms and conditions which prohibit relevant harmful material, do</p>	

<p>you have any comments on Ofcom’s view that effective protection of users is unlikely to be achieved without having this measure in place and it being implemented effectively?</p>	
<p>Question 4: Do you have any comments on Ofcom’s view that, where providers have terms and conditions requiring uploaders to notify them if a video contains restricted material, additional steps will need be taken in response to this notification to achieve effective protection of under-18s, such as applying a rating or restricting access?</p>	<p>4.20 offers providers two routes to compliance in relation to restricted material uploaded to the service –</p> <p>“it is unlikely that effective protection of under-18s can be achieved without the provider taking the additional step of either notifying viewers where a video contains restricted material or restricting access to it by under-18s.”</p> <p>This implies that it can be sufficient merely to notify viewers that a video they are accessing contains restricted material but that is it not necessary to restrict access to it by under 18s. This does not clearly align with what follows so could be confusing to services trying to do the right thing.</p> <p>4.21 offers the same choice again between either rating mechanisms OR access control</p>
<p>Question 5: Do you have any comments on the draft guidance about reporting or flagging mechanisms, including on Ofcom’s view that reports and flagging mechanisms are central to protecting users?</p>	
<p>Question 6: Do you have any comments on the draft guidance about systems for viewers to rate harmful material, or on other tagging or rating mechanisms?</p>	<p>4.85 begins to address the concerns above as it states “For material which has the most potential to harm under-18s we would not expect a rating system on its own to be a sufficient measure and in our view this will need to be linked to access control measures.”</p> <p>So this may raise the difficult question of what material has the most potential to harm under-18s. This can be interpreted to suggest that some R18 certificate or unsuitable for classification materials could still fall short of the bar where access control measures are required – but that does not appear to be Ofcom’s intention elsewhere in the document.</p> <p>It would perhaps be less ambiguous to state that all restricted material requires access control measures EXCEPT for other material that might impact the development of under-18s only if the risks and harms are arguably low enough to justify alternative measures.</p>
<p>Question 7: Do you have any comments on the draft guidance about age assurance and age verification, including Ofcom’s interpretation of the VSP Framework that VSPs containing pornographic material and material unsuitable for classification</p>	<p>4.87 – Please note: the method referred to as “face-recognition biometrics” is mis-named. There is no recognition involved (except if that is used later for the purpose of authenticating the user and the same individual who has previously been age verified). This should be renamed “Facial age estimation”</p> <p>4.87 and 4.88 Facial age estimation is a good example of the challenge with these new definitions – all forms of biometric age estimation have the capability of providing very high levels</p>

must have robust age verification in place?

of assurance about a user's age – to the legal standard “beyond reasonable doubt” if the age they test for is sufficiently greater than the age being enforced. So, using facial age estimation where artificial intelligence is determining if the user appears to be over 25 will be accurate in excluding under-18s 99.99% of the time. A level of certainty that provides enforcement standards which far exceed those of your average off-licence, and can be quite reasonably considered as providing “age verification” in this scenario.

We recommend the use of the term “age verification” which can be achieved to different “levels of assurance”. Those levels depend on a range of factors – referred to as “vectors of trust” in BSI standard PAS 1296:2018.

This is not a critical change to the guidance, but is an important fact in understanding the technology and therefore suitability as control mechanisms for different situations.

4.89

Please note: We are unaware of any age estimation method based on retinal patterns. These may be used for recognition (is this the same user I saw yesterday) but we have not heard of any theoretical, experimental or commercial examples. Please send them our way if you have.

Fingerprints are not much better as an example (Turkish researchers secured 83-93% accuracy in a sample of 50 fingers in 2014 but this is the only reference to this technique in the context of age verification as defined in this situation)

You may prefer to suggest “facial image, voiceprint and text analysis.” (but as linguistic analysis is used below, text would be duplicative here)

g) it is unclear to us what is meant by “Password-protected content” – this is not a method AV or AV but may refer to an authentication mechanism to confirm a user is one who has been previously verified? As such, does it sit within this list or is it a separate but important point about authentication – the process of confirming an individual is the rightful owner of the evidence or a record of that evidence of age.

4.91 “This is likely to be of greater consideration for age assurance and age verification measures” is in danger of repeating an unjustified trope that AV is somehow inherently a threat to privacy and data security. While this was a strong campaigning tactic for its opponents, it was never substantiated in fact, given AV providers are subject to GDPR, and in most cases, go further with IS27001, the BBFC's AV Certification Scheme, and compliance with the AVPA code of conduct. Indeed, privacy concerns may arise with reporting, rating, tagging, and parental controls

5.23 “VSP providers should have regard to Section 3 where we set out the types of content likely to be considered as relevant harmful material and restricted material”. We read Section 3 as going further than setting out content *likely* to be considered as

	<p>such? We read it to be definitive e.g. 3.4 “Harmful Material encompasses restricted material and relevant harmful material.” And then goes on to define Restricted material specifically.</p>
<p>Question 8: Do you have any views on the practicalities or costs relating to the implementation of robust age verification systems to prevent under-18s from accessing pornographic material and material unsuitable for classification? Please provide evidence to support your answer wherever possible.</p>	<p>5.14 “We understand that some of the most sophisticated measures set out in Section 4 may only be practicable and proportionate for the largest platforms.” We believe that this phrasing mischaracterises the maturity of the open and highly competitive market for age verification services, making AV universally available for services, regardless of resource levels, staffing or size. Age checks cost pence not pounds (some providers publish their tariff) and pricing is well below the cost of identity checks used for “know your customer” rules etc. This paragraph may inadvertently put services off from exploring the AV options available to them. Perhaps it could be rephrased to accept that more complex or novel AV techniques may not be viable for services with limited resources, but there are widely available, off-the-shelf AV services, many offered as easily integrated plug-ins to the major platforms services are built on.”</p> <p>4.100 Relying on publicly available sources or otherwise easily known information such as name, address and date of birth to verify the age of a user” - We note that this is considerably more restrictive than the proposed requirement from the previous regulator (BBFC) and will create a significant regulatory burden well above that envisaged under the Digital Economy Act. While providers operate counter-measures against fraudulent use of their services e.g. surveillance for contra-indicators such as multiple use of the same credential, the level of assurance thought necessary for access to porn was set relatively low. Perhaps “solely” could be added after “Relying” to give some latitude to use electoral roll data, for example, provided some additional counter-fraud measures are in place.</p> <p>More generally, we would ideally wish to see Ofcom’s guidance making reference to achieving a level of assurance defined based on BSI PAS 1296:2018 or equivalent, to encourage services and suppliers to adopt a common language and understanding of standards as this area of regulation evolves.</p>
<p>Question 9: Do you have any comments on the draft guidance about parental control systems?</p>	<p>4.108 e “Trust-based measures such as parental controls may provide alternative and lower-risk forms of authentication and verification for under-18 users” - Our understanding of the political motivation for the change to the AVMSD is that parents have not been making use of parental controls, and they are not completely effective on their own.</p> <p>Parental controls have a complementary role to play alongside age verification but should not be mistaken for an alternative when better technical approaches are widely available that do not rely on the knowledge of and ability to make use of parental controls amongst parents.. There is a risk the guidance may give that impression in places.</p>
<p>Question 10: Do you have any comments on the draft</p>	<p>The service’s complaints process needs to include and ideally integrate with any third party e.g. an AV provider so there</p>

<p>guidance about the measure regarding complaints processes or on the regulatory requirement to provide for an impartial dispute resolution procedure?</p>	<p>needs to be an obligation to select only third party suppliers who offer such a process. (AVPA members must rectify errors under our code of conduct)</p>
<p>Question 11: Do you have any comments on the draft guidance about media literacy tools and information?</p>	
<p>Question 12: Do you have any comments on the with the draft guidance provided about the practicable and proportionate criteria VSP providers must have regard to when determining which measures are appropriate to take to protect users from harm?</p>	<p>In preparing previously for the introduction of AV for pornography – but this is a more general point – there was general acceptance and even in many cases support for the concept but a great concern that it would be unevenly implemented and enforced, with disproportionate attention paid to a limited number of high profile services; this would lead to rapid diversion of traffic to sites escaping the attention of the regulator.</p> <p>On a related point, the scope for services to interpret this guidance very differently is narrowed by its publication (particularly clear in A 1.4) but there is still considerable breadth in the choices open to services as they plan compliance. The risk is of a race to the bottom, with services that take a more responsible approach, finding themselves undercut’ but competitors and then forced to lower their own standard. So, early benchmarks setting some lines in the sand will allow services to coalesce relatively closely around a median. The risk is service A is very strict; service B takes a more liberal attitude; customers migrate form A to B until A simply imitates the liberal approach B adopted. If both were told “for the sort of content you have on offer, Ofcom would expect services to implement age verification to a Medium level of assurance by which we mean (then define medium in PAS 1296 terms).</p> <p>6.20 It may be helpful to mention the Age Verification Providers Association website as a source of advice on the latest methods available for age assurance and age verification, and guidance to the main sectors on which AV solutions may be most appropriate. AV providers can also provide advice to services based on their existing design, functionality and data as to which approach to adopt.</p>
<p>Question 13: Do you have any comments on the draft guidance about assessing and managing risk?</p>	
<p>Question 14: Do you have any comments on the impact assessment in Annex 1, including the potential impacts to VSPs outlined in tables 1 and 2, and any of the potential costs incurred (including any we have not identified)?</p>	

Question 15: Do you have any comments on our provisional assessment that the potential costs for providers are proportionate to achieve the regulatory requirements of the regime?

It is worth adding the economy of scale that will emerge through the cumulative impact of legislation - AVMSD, GDPR, Age Appropriate Design Code and the Online Safety Bill all encourage the adoption of universal age assurance by services which pose any degree of harm to children, enter into contracts with their users (including agreement to terms and conditions) or process data based on user consent. Through the international interoperability being developed for both age verification and parental consent, the cost burden of compliance with age-related regulations will fall rapidly.

Question 16: Do you have any comments on any other part of the draft guidance?