Your response

Questions for industry	Your response
Question 1: Are you providing a UK-established service that is likely to meet the AVMSD definition of a VSP? **Please provide details of the service where relevant. The establishment criteria under the AVMSD are set out in annex 5.**	Confidential? – Y / N
Question 2: Is your service able to identify users based in specific countries and do you provide customised User Interfaces (UI), User Experience (UX) functionality or interaction based on perceived age and location of users?	Confidential? – Y / N
Question 3: How does your service develop and enforce policies for what is and is not acceptable on your service? (including through Ts&Cs, community standards, and acceptable use policies) **In particular, please provide information explaining:** • **what these policies are and whether they cover the categories of harm listed in the AVMSD (protection of minors, incitement to hatred and violence, and content constituting a criminal offence – specifically Child Sexual Exploitation and Abuse, terrorist material, racism and xenophobia);** • **how your service assesses the risk of harm to its users;** • **how users of the service are made aware of Ts&Cs and acceptable use policies; and** • **how you test user awareness and engagement with Ts&Cs.**	Confidential? – Y / N
Question 4: How are your Ts&Cs (or community standards/ acceptable use policies) implemented?	Confidential? – Y / N

In particular, please provide information explaining: • **what systems are in place to identify harmful content or content that may breach your standards and whether these operate on a proactive (e.g. active monitoring of content) or reactive (e.g. in response to reports or flags) basis;** • **the role of human and automated processes and content moderation systems; and** • **how you assess the effectiveness and impact of these mechanisms/ processes.**	
Question 5: Does your service have advertising rules? **In particular, please provide information about any advertising rules your platform has, whether they cover the areas in the AVMS Directive, and how these are enforced. See Annex 5 for a copy of the AVMSD provisions.**	Confidential? – Y / N
Question 6: How far is advertising that appears on your service under your direct control, i.e. marketed, sold or arranged by the platform? **Please provide details of how advertising is marketed, sold and arranged to illustrate your answer.**	Confidential? – Y / N
Question 7: What mechanisms do you have in place to establish whether videos uploaded by users contain advertising, and how are these mechanisms designed, enforced, and assessed for effectiveness?	Confidential? – Y / N
Question 8: Does your service have any reporting or flagging mechanisms in place (human or automated)? **In particular, please provide information explaining:**	Confidential? – Y / N

• **what the mechanisms entail and how they are designed;** • **how users are made aware of reporting and flagging mechanisms;** • **how you test user awareness and engagement with these mechanisms;** • **how these mechanisms lead to further action, and what are the set of actions taken based on the reported harm;** • **how services check that any action taken is proportionate and takes into account Article 10 of the European Convention of Human Rights (freedom of expression);** • **how users (and content creators) are informed as to whether any action has been taken as a result of material they or others have reported or flagged;** • **whether there is any mechanism for users (including uploaders) to dispute the outcome of any decision regarding content that has been reported or flagged; and** • **any relevant statistics in relation to internal or external KPIs or targets for response.**	
Question 9: Does your service allow users to rate different types of content on your platform? **Please provide details of any rating system and what happens as a result of viewer ratings.**	Confidential? – Y / N
Question 10: Does your service use any age assurance or age verification tools or related technologies to verify the age of users? **In particular, please provide information explaining:** • **how your age assurance policies have been developed and what age group(s) they are intended to protect;** • **how these are implemented and enforced;** • **how these are assessed for effectiveness or impact; and** • **if the service is tailored to meet age-appropriate needs (for example, by**	Confidential? – Y / N

restricting specific content to specific users), how this works.	
Question 11: Does your service have any parental control mechanisms in place? **In particular, please provide information explaining:** • **how these tools have been developed;** • **what restrictions they allow;** • **how widely they are used; and** • **how users of the service, and parents/ guardians if not users themselves, are made aware of and encouraged to use the parental control mechanisms that are available.**	Confidential? – Y / N
Question 12: Does your service have a complaints mechanism in place? Please describe this, including how users of your service can access it and what types of complaint they can make. **In particular, please provide information explaining:** • **any time limits for dealing with complaints;** • **how complainants are informed about the outcomes of complaints;** • **any appeals processes, how they work, and whether they are independent from the complaints processes; and** • **the proportion of complaints which get disputed or appealed.**	Confidential? – Y / N
Question 13: What media literacy tools and measures are available on your service? **In particular, please provide any relevant information about:** • **how you raise awareness of media literacy tools and measures on your service;** • **how you assess the effectiveness of any media literacy tools and measures provided on your service; and** • **how media literacy considerations, such as your users' ability to understand and respond to the**	Confidential? – Y / N

content available to them feature in your thinking about how you design and deliver your services, for example in the user interfaces, flagging content and use of nudges.	
Question 14: Do you publish transparency reports with information about user safety metrics? **Please provide any specific evidence and examples of reports, information around the categorisation and measurements used for internal and external reporting purposes, and whether you have measures in place to report at country/ regional level and track performance over time.**	Confidential? – Y / N
Question 15: What processes and procedures do you have in place to measure the impact and effectiveness of safety tools or protection measures? **If not already captured elsewhere in your response, please provide information relevant to all of the measures listed above explaining:** • **how you test and review user awareness and engagement with each measure (including any analysis or research that you would be willing to share with Ofcom);** • **how often policies and protection measures are reviewed, and what triggers a review; and** • **how you test the impact of policies on users and the business more generally, such as how you balance the costs and benefits of new tools.**	Confidential? – Y / N
Question 16: How do you assess and mitigate the risk of inadvertent removal of legal or non-harmful content? **In particular, please provide any information on:** • **how freedom of expression is taken into account during this assessment;** • **how appeals are handled and what proportion are successful; and**	Confidential? – Y / N

• **audits of automated removal systems and, if you have them, any metrics that relate to their effectiveness.**	
Question 17: Have you previously implemented any measures which have fallen short of expectations and what was your response to this? **Please provide evidence to support your answer wherever possible.**	Confidential? – Y / N
Question 18: How does your service develop expertise and train staff around different types of harm? (e.g. do you have any partnerships in place?)	Confidential? – Y / N

Questions for all stakeholders	**Your response**
Question 19: What examples are there of effective use and implementation of any of the measures listed in article 28(b)(3) the AVMSD 2018? **The measures are terms and conditions, flagging and reporting mechanisms, age verification systems, rating systems, parental control systems, easy-to-access complaints functions, and the provision of media literacy measures and tools. Please provide evidence and specific examples to support your answer.**	Confidential? – N Over one billion children are online, equivalent to one in three internet users worldwide.[1] This was before the Covid-19 pandemic, during which there has been a global surge in the number of young people using digital technologies.[2] But, the digital world is built by adults, for adults without children in mind. This means that children are treated as adults online, by design and default. The digital environments that are so central to children's lives fail to anticipate their presence or provide a service that ensures that they are protected. This means a lack of protection from harmful and illegal content and system level design decisions that expose children to a range of risks in addition to content[3]. Consequently, there are limited examples of the *'effective use and implementation'* of the measures listed in 28(b)(3). It is noteworthy that the examples of effective use and implementation we identify here correspond to digital services designed with children as the end user, and their best interests, in mind. This is insufficient as we know that children do not only use 'child-directed services' and enjoy using

[1] One in Three: Internet Governance and Children's Rights, Sonia Livingstone, John Carr and Jasmina Byrne. January 2016, Unicef.

[2] Everyone is a kids and family brand now Data, observations and recommendations for companies interacting with kids and families during Coronavirus, page 5. April, 2020. Super Awesome.

[3] Risky-by-Design by 5Rights Foundation, 2020.

mixed audience platforms, in some cases more than the child offering. YouTube is a clear example of this. 53% of 8 to 12 year-olds say YouTube is the site they watch "the most," compared to just 7% for YouTube Kids.[4] Such evidence is also indicative of the current failure of age verification (Article 28(b)3.(f)) systems given that the minimum age for using YouTube is 13.

The popularity of VSPs among children (Ofcom itself notes that 98% of children aged 8-15 who use the internet have used a VSP in the past year[5]) means that VSPs have a responsibility to ensure the safety and rights of children. A responsibility that should be enforced by the regulator.

Call on the regulator to require VSPs to conduct child impact assessment

It would be practical and proportionate for Ofcom to require all VSPs to assess the risks that their service presents to children *before* products are released and when they are updated in the form of child impact assessments. The measures listed in AVMSD 28(b)(3), should form the minimum against which VSPs are assessed as part of child impact assessments. Beyond these measures, VSPs should consider all design features specific to the service, how these interact and whether service design exposes children to inappropriate content, contact, conduct or commercial/contract pressures.

AVMSD 28(b)3. suggests a selective approach as *'the appropriate measures shall be determined in light of the nature of the content in question.'* A proportionate and risk-based approach is necessary at the stage of implementation, however consideration of *all* of the measures at the design stage of all VSPs should be mandatory. This is because we know that change to discreet areas of service and retrofitting solutions results in sporadic change that fails to ensure young people's safety by design and default.

For example, TikTok might have made substantial changes to their community guidelines[6] detailing content that is prohibited from the platform but the TikTok algorithm has since been found to actively promote prohibited content, a video of a user taking his own life. Children report being actively recommended the video on their algorithmically generated 'For You' page.[7] Further still, the video is being actively recommended to children as it has been spliced and embedded into videos of kittens and puppies, which children are likely to see.[8] Though TikTok admitted failings, promising to make changes to content take-down processes in the future, there remains a failure to approach the issue of content spread and amplifi-

[4] https://www.commonsensemedia.org/user/register?destination=/research/the-common-sense-census-media-use-by-tweens-and-teens-2019 p.4
[5] Ofcom, Online Nation 2020 Report, 23 June 2020
[6] New Rules, Who Dis: TikTok Overhauls Its Community Guidelines Wired, 8Th January 2020
[7] TikTok tries to remove widely shared suicide clip, BBC News. September 8th, 2020.
[8] TikTok tries to remove widely shared suicide clip. BBC News, 8th September 2020.

cation at the level of the algorithm. Instead moderators are left chasing individual pieces of content against the clock and against the algorithm, to prevent high numbers of views.

Given the large number of children on TikTok[9], this would clearly fall short of the *'appropriate measures'* an AVMS should take to protect minors from harmful content as required by the Directive.[10] Assessing the risk of the algorithmic systems that govern which content is promoted to children and how, should be captured in a child impact assessment, above and beyond ensuring the measures defined in AVMSD 28(b)3 are met.

To build the digital world that young people deserve, it is vital that the systems that touch upon these measures, for example recommendation algorithms, are also part of the regulator's consideration of compliance with the Directive.

Examples of effective use and implementation:

Terms and conditions

The BBC Own it app offers age appropriate terms and conditions in so far as these are presented in a clear, concise and accessible way.[11] For terms and conditions to be effective for children, in addition to being clearly presented published terms must deliver the following.

- **Provide accessible Information via:** multiple formats, with prominent key terms and simplified language which has been tested with diverse children, addressing diverse audiences and ensure the veracity of information contained in published terms so that platforms in practice clearly say what they do and do what they say.
- **Ensuring redress by:** enabling transparent reporting, providing expert advice, and swift response times to users.
- **Establish standardised frameworks by:** setting clear expectations, ensuring there are clear consequences when published terms are breached, normalising the need to establish children's evolving capacity to understand published terms, establishing industry codes, regulation, standards and certification, and mitigating commercial interest.
- **Prevent children from being 'nudged' by:** Creating age appropriate design norms, introducing regulation, ensuring appropriate

[9] According to research by Qustodio, 17.7% of all UK children reported using TikTok prior to the pandemic. This number has likely increased since then.
[10] Article 6a, AVMSD
[11] BBC Own it: Privacy Notice

	timing of consent, mitigating the prioritisation of commercial interests and a failure to recognise a child as a child. 5Rights Foundation is currently working with the IEEE to develop a standard that digital service providers will be able to use to assess whether or not terms and conditions are age appropriate.[12] **Rating systems** BBC iPlayer Kids tailors the content available to children depending on the child's age entered on set up.[13] Following established rating systems set out by BBFC[14] both BBC iPlayer and their child-directed service BBC iPlayer Kids set clear expectations with prior warnings about the kinds of content that users will view, with pop-ups for all users, not only children. This is a rare exception as the majority of the digital world fails to impose offline protections online. Buying age-restricted items, for example alcohol, requires identification and in the offline world there are physical barriers such as identification to prevent children from doing so. Digital environments are not only failing to rate content, but actually makes it easy for children to access age inappropriate and illegal products. For example, an investigation by the BBC revealed how easy it was to access drugs via social media, including popular VSP Snapchat.[15] **Parental Control Systems** Netflix allows users to set up different profiles for each user under one account, with the means to designate an account as for a young person.[16] Individual profiles can be subject to personalised maturity ratings requirements, and the Netflix 'kids' profile removes access to account settings and only recommends content that is age-appropriate. Netflix's parental controls are a form of mitigating risk of children being exposed to age-inappropriate content. Unfortunately, too often, parental control systems operate under surveillance models. For example, Facebook's Messenger for Kids platform allows parents to download messages[17] their children send and receive via the service, including images and videos. These 'surveillance' models do little to mitigate risk and only allow for intervention *after* a harm has occurred.
Question 20: What examples are there of measures which have fallen short of expectations regarding users' protection and why?	Confidential? – N As mentioned in response to Questions 19 & 22, VSPs should be required to undertake a child impact assessment so that risks facing children are

[12] This work is currently in progress. For more information see 5Rights Foundation's website.
[13] BBC iPlayer Kids - What content is available in the app? Accessed September, 2020.
[14] BBFC launches new Classification Guidelines and calls for greater age rating consistency across online channels, January 2019.
[15] Newsbeat has been investigating how social media is being used to sell drugs. 18th August, 2020.
[16] Netflix, 'Parental controls on Netflix.'
[17] Facebook, 'Giving Parents Even More Control in Messenger Kids,' February 2020

Please provide evidence to support your answer wherever possible.	anticipated and mitigated *before* products and services are distributed, and on an on-going basis. This will inform *'their own assessment of the risk of harm'* which, as described in 2.28 will inform which measures are appropriate and proportionate. This is a necessary step so that VSPs are not able to pick and choose from measures, when all measures should be considered in advance when children are anticipated on the service. While recognising the importance for appropriate and proportionate action, Ofcom should require all VSPs to implement robust, privacy preserving age verification tools on services where children may be able to access pornography and other harmful content.[18] After establishing a child's age, the service should be tailored to the developmental capacity and vulnerability of the child. **Age verification systems** Without establishing the age (or age range) of users, many service providers will find it difficult to give children the specific protection to which they are entitled.[19] A proportionate and 'risk-based' approach to age assurance – similar to that introduced by the Age Appropriate Design Code[20] means that the level of certainty that a service must obtain about the age of their users will depend on a range of factors. The circumstances in which VSPs need to establish the age of users can only be established once the service has answered truthfully, fairly, and transparently the following three questions: • In what ways does my service or product impact on children? • How can I mitigate any risk? • How could I amplify or build in any benefits? The legitimate answers may be (in turn) that a service or product doesn't impact children, there is no risk to children, and that a service is such that it cannot benefit children. If that is the case, AV/AS would be unnecessary. Such examples could include an academic website, a hardware supplier, an estate agent that would not foresee their services being impacted by the presence of children. However, for a vast number of digital services, including VSPs that enable access to content that may be inappropriate or harmful to children, and indeed enables children to create, upload and livestream their own content alongside a range of design features that enable contact with other unknown (potentially adult) users, these answers are quite different. Checking which of their users are children, VSPs would be able to make special provision that mitigates against any foreseeable risk, and, take

[18] Article 6(a)(1)

[19] The United Nations Convention on the Rights of the Child. November, 1989.

[20] Age appropriate design: a code of practice for online services, Information Commissioners Office. June, 2020.

measures to prevent harm whilst offering support and redress in the event that harm happens. This would enable VSPs to offer a distinct/bespoke service for children that upholds their rights in a designated space or user experience. Bespoke design features have already started to be introduced, for example TikTok has disabled private messaging for under 16's on the service.[21] The potential positive impact of this intervention, brought about due to safety concerns, is undermined when the platform cannot verify which users are under 16 and require this setting.[22] Adequate and proportionate age verification is both about enabling young people to access the very best bespoke user experience in addition to preventing children from accessing some content all together as in the case of pornography.

It is evident that self-declaration, the norm for many social media sites, is not working. For example, Snapchat have admitted that their age verification systems are ineffective.[23] Twitch, which also relies on self-declaration of user's date of birth, enables children to livestream and connect with other users in real time and has been found to expose children under the age of 13 to inappropriate messages from anonymous chat participants.[24] VSPs with weak age verification systems enable children to gain access to the service underage or/and allow adult to pose as children. Via these services, children may encounter inappropriate or harmful content.

Age verification is also vital if published terms are to be upheld and enforced by VSPs. Research by Ofcom shows that, TikTok was the most downloaded app amongst children last year, particularly among 10-12 year old girls with 31,000 downloading the app during the last quarter of 2019.[25] This is despite the minimum age to use TikTok being stated as 13. A lack of regulatory oversight has meant that VSPs are not only aware that users under the age of 13 are on their platform, they are able to publicly acknowledge this with little or no consequence despite exposing children to illegal and harmful content on the platform.[26]

Despite age verification being an active area of innovation, the methods that are widely used are ineffective. Ofcom has a primary role in ensuring that companies use robust and risk-based age verification systems that are privacy-enhancing and easy for children to engage with and the information gathered to assess the age of a child must not be used, stored or shared for any other purpose.

Terms and conditions

[21] TikTok introduces Family Pairing. By Jeff Collins, Trust and Safety, TikTok. April 2020.
[22] TikTok bans under-16s from private messaging BBC News, April 2020.
[23] Snapchat admits its age verification system does not work. The Independent, 19th March 2019.
[24] Children Stream on Twitch—Where Potential Predators Find Them. Wired. 30th July 2020.
[25] Half of British children use TikTok regularly despite safety fears, study shows. The Telegraph, 24th June 2020.
[26] A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions. The New York Times, 17th September 2020.

In addition to upholding minimum age requirements, published terms also need to say what they do and do what they say in relation to harmful and illegal content. It is evident that this is not happening at the moment, with countless cases of content officially prohibited on the platform remaining on the service and, further still, being amplified by recommendation systems. For example, YouTube has stated that the platform will do more to tackle the spread of medical misinformation, by banning this kind of content. Since then, misleading videos have been viewed more than 62 million times on YouTube.[27]

See also response to question 19.

Flagging and reporting mechanisms

In addition to allowing content to be promoted despite being banned by the platform, children are exposed to inappropriate content via direct messaging. Flagging and reporting mechanisms should be robust across all aspects of the service, not only uploaded videos. Former content moderators at TikTok revealed that children are currently being put a risk due to a prioritisation of 'flagged videos' ahead of reported private messages resulting in a backlog of over 1000 messages. This is despite the fact that moderators estimated that around 1 in 10 private messages flagged were due to adults messaging children inappropriately, sometimes with as many as 10 different adults messaging one child.[28] Flagging and reporting mechanisms are redundant if, as in this case, timely action is not taken when content is flagged.

Easy-to-access complaints functions

Many VSPs do not offer straightforward and age-appropriate complaints functions for users to address breaches of published terms or other things occurring on the platform. For example, Instagram does not provide adequate redress when users flag content. In cases where content promoting eating disorders were reported by users, users described not being notified of what happened next.[29] Similarly, when users flagged posts of children in bathing suits where adults have commented inappropriately below, complaints were left unresolved.[30] Instagram does not have a transparent reporting and flagging process, and often there is insufficient action.

Require transparency, particularly in relation to algorithmic recommendation systems

Currently VSPs are not obligated to share the details of how their systems work, despite serving up harmful content to children. Some VSPs have said they are willing to *"disclose their algorithms, moderation policies, and data flows to regulators"*[31] but this is used

[27] Coronavirus: False claims viewed by millions on YouTube. BBC News, May 14th 2020.
[28] Revealed: How TikTok banned paedophiles for just a week if they are caught messaging children. The Telegraph, 19th July 2020.
[29] Online eating disorder 'trigger' crack-down call BBC News, June 22nd 2020.
[30] 'Sexy girl': How Instagram allows the offering of young girls as fetishised flesh. Collective Shout, September 13th 2019.
[31] Why it matters that TikTok wants to reveal its algorithms, by Rebecca Heilweil. Vox, 29th July 2020.

	as a carrot to pressure competitors rather than a requirement to improve transparency and, ultimately, user safety. It is incumbent on the regulator to ensure that the current imbalance of power between VSPs and their user base, a large proportion of which are children, is somewhat restored. A focus on content take down, as opposed to *how* content comes to be recommended and amplified to users of VSPs, many of whom are children, has not served to protect children from harmful nor illegal content. A content take down model to regulation is always, by necessity, after the fact and is, particularly for children who may have come into contact with that content, too late. A failure to address risks systemic in the design of VSPs renders parents and children powerless, even when parental control systems and media literacy are provided. **Parental control systems** Parents play an important role in their children's digital lives. Parental controls however are insufficient without additional accompanying measures. This is because it is design decisions made by VSPs that dictate how easy it is to circumvent age restrictions when joining the platform and what children can see and do on the platform. For example, Instagram announced policy changes to clamp down on content depicting self-harm and suicide[32] yet, almost a year later, an investigation revealed over 120,000 relevant posts discoverable under relevant hashtags.[33] The fact that, in this case, Instagram has failed to uphold their published terms is not the responsibility of parents or indeed teachers and even children themselves. Instagram provides 'Tips for parents' [34] falling short of parental control systems. Ironically, these tips include guiding parents through how to aid their child to turn privacy settings from public (default) to private. The fact that children's profiles are public by default on Instagram (and many other VSPs[35]) is a prime example of where, even if more robust parental systems were in place, parents are ultimately powerless to design decisions that put young people at risk via design features. It is the regulator's role to hold VSPs to account to ensure that digital products and services are fit for purpose and prioritise the safety and best interests of young people.
Question 21: What indicators of potential harm should Ofcom be aware of as part of its	Confidential? – N **Access to adult content**

[32] Changes We're Making to Do More to Support and Protect the Most Vulnerable People who Use Instagram by Adam Mosseri, Instagram Blog, 7th February 2019.

[33] Instagram failing to delete thousands of suicide posts. The Times, 22nd January 2020.

[34] Know how to talk with your teen about instagram: a parent's guide, accessed September 2020.

[35] Facebook, Instagram, TikTok, Twitch, YouTube all have default settings that render children's account profiles and information uploaded public by default.

ongoing monitoring and compliance activities on VSP services? **Please provide evidence to support your answer wherever possible.**	In addition to the range of content that 2.25 outlines VSPs will need to have appropriate measures in place to protect children from, Ofcom needs to ensure that robust age verification is mandatory for all VSPs where children can access adult content. Government committed to including age verification in the Online Harms Bill, in lieu of a former commitment to make age verification on pornography sites mandatory under the Digital Economy Act, 2017.[36] It is vital that Ofcom ensures age verification on pornography sites, and indeed any site where children might access porn. This includes social media sites as 46% of young people who watch porn do so via social media, with 44% choosing traditional porn websites. Evidence from BBFC also confirms that the majority of young people's first-time watching pornography was accidental, with over 60% of children 11-13 who had seen pornography saying their viewing of pornography is unintentional.[37] **Indicators of potential harm** Ofcom should be aware of how design features that may not immediately appear connected to harmful or illegal content can interact to increase the risk of potential harm for children on VSPs. For example, the ability for children to broadcast live from intimate spaces such as bedrooms can allow groomers to gain an insight into a child's hobbies and interests. Evidence shows that such information is used to establish a rapport and build a relationship.[38] To be an effective regulator, Ofcom must ensure that the preparatory stages of grooming are part of mandatory, ongoing monitoring and compliance. Alongside children's accounts getting recommended to unknown adults on VSPs[39] design features that are common on VSPs facilitate the grooming of children and the creation of new CSAM. For example, live chat functions allow viewers to interact with children in real-time and make requests of them.[40] Among children who livestreamed, 6% received requests to change or remove their clothes, according to the NSPCC. [41] Similarly, features that may appear to have little to do with content, can nudge children towards risky behaviour. IWF report children as young as 7 years old have been pressured into performing specific sexual acts on livestreaming platforms in exchange for "likes".[42]

[36] Online Harms: Statement made on 16 October 2019, Statement UIN HCWS13. Nicky Morgan, Former Secretary of State for Digital, Culture, Media and Sport.

[37] Children see pornography as young as seven, new report finds. BBFC, 26th September 2019.

[38] Nuria Lorenzo-Dus, Cristina Izura, Rocío Pérez-Tattam, Understanding grooming discourse in computer-mediated environments, Discourse, Context & Media, Volume 12, 2016, Pages 40-50, https://doi.org/10.1016/j.dcm.2016.02.004.

[39] On YouTube's Digital Playground, an Open Gate for Pedophiles. NY Times, June 3rd 2019.

[40] NSPCC: Livestreaming and video-chatting. Snapshot 2.

[41] According to research from NSPCC, 24% of primary school children have encountered something that has made them uncomfortable on a livestreaming platform, 6% have been asked to remove their clothing, and 8% have seen someone without all their clothes. For secondary school children, 11% have encountered something that has made them uncomfortable, 5% have been asked to remove their clothing, and 7% have seen someone not wearing all their clothes. NSPCC also reports 24% of all school children having livestreamed before, indicating a substantial number of young people actively at risk of encountering inappropriate or harmful content.

[42] The why, the how, the who and the results. IWF Annual Report, 2019.

	Ofcom should ensure that VSPs uphold their published terms (see examples provided in response to questions 19 & 20) as this would help to incentivise VSPs to obey minimum age limits and protections against adult/child interaction.[43] This would also be vital for holding platforms accountable for content that their own community guidelines claim not to allow, including self-harm and suicide content, which is being promoted to young people via algorithms.[44] By mandating that VSPs undertake child impact assessments against all of the measures (AVMSD 28(b)(3)) Ofcom would ensure that indicators of potential harm in relation to content were a core part of the monitoring and compliance. Most crucially, this would go a long way towards enforcing that VSPs are safe by design and default for young people. For more information about design features that pose a risk to children and that are embedded within many VSP services including livestreaming services see https://www.riskyby.design.
Question 22: The AVMSD 2018 requires VSPs to take appropriate measures to protect minors from content which 'may impair their physical, mental or moral development'. Which types of content do you consider relevant under this? Which measures do you consider most appropriate to protect minors? **Please provide evidence to support your answer wherever possible, including any age-related considerations.**	Confidential? – N **Types of content:** • Age-inappropriate content, pornography, extreme and real-life violence, discriminatory or hateful content, disinformation, misinformation, content that endorses risky, harmful or unhealthy behaviours such as anorexia, self-harm, suicide **Clearly designated advertisement content** Advertising is currently not being marked clearly. For example, on VSP Twitch, US Military recruiters have been found to covertly recruit streamers under the age of 18. Users have been invited to enter "giveaway" but when they follow the link to the giveaway form, it leads users to a military recruitment form.[45] Relatedly, children have a difficult time understanding the role of advertising in vlogging content on popular sites like YouTube making it difficult to decipher when vloggers are advertising their own merchandise.[46] **Measures most appropriate to protect minors:** In addition to the measures outlined in AVMSD 28(b)(3), as an effective regulator, Ofcom should mandate that VSPs conduct a child impact assessment that anticipates the risks facing children on VSPs *before* products and services are distributed, and on an on-going basis. This would

[43] Growing Up Online Connected Kids. By Kaspersky Lab. April, 2016. One in three young people lie about their age online, pretending to be older.
[44] https://www.wired.com/story/when-algorithms-think-you-want-to-die/
[45] Twitch tells US Army to stop sharing fake prize giveaways that sent users to recruitment page. The Verge, 17th July 2020.
[46] YouTube's child viewers may struggle to recognise adverts in videos from 'virtual play dates' by Rebecca Mardon, LSE Blog, 25th September 2019.

	include design decisions that shape the algorithmic recommendation of content. As discussed at length in response to Question 24, Ofcom's focus should not only be on individual pieces of content which are inappropriate to children in the digital environment. Such content will always exist in some form, though the regulator must act to address the amplification of illegal and harmful content via recommendation systems. By mandating VSPs to undertake child impact assessments before rolling out new services, features, or upgrades, VSPs will then need to satisfy the regulator that any risks to children have been mitigated by design. *Providers of regulated services therefore must:* • conduct a Child Impact Assessment in relation to their services (and individual features) in order to identify the risks that their operation or use may pose to young people; • take measures to minimise or eradicate any risks identified in the Child Impact Assessment; • keep a record of the Child Impact Assessment and any action taken as a result; • regularly review the Child Impact Assessment and the effectiveness of any risk-mitigation measures taken; • make available to the regulator any data used to inform the Child Impact Assessment and the action taken as a result, and collect and provide data on the effectiveness of the action taken; • inform the regulator of any emerging concerns, including those that may have industry-wide relevance; and • have regard to any guidance on Child Impact Assessments produced by the Regulator.
Question 23: What challenges might VSP providers face in the practical and proportionate adoption of measures that Ofcom should be aware of? **We would be particularly interested in your reasoning of the factors relevant to the assessment of practicality and proportionality.**	Confidential? – N Protecting the safety of young people online, that is all internet users under the age of 18, and upholding the full range of their rights is simply the price of doing business in today's digitally mediated world. The practical and proportionate adoption of measure will require adjustments to the business model. That is, VSPs and all online services must prioritise the best interests of children above profit. Building in child protection by design and default has the potential to significantly reduce the long-term costs of inaction. The issues that young people currently face

	online do not stay online. They impact on schools, social services, the criminal justice system and the NHS, as young people have record levels of self-harm, eating disorders, and anxiety and increasing numbers are subject to online sexual abuse and exploitation. From the perspective of design, retrofitting technical solutions is undesirable for young people and for business. This approach fails to realise the benefits of systemic change, and responding to harm on an ad hoc basis is not financially desirable. There may always be cases where young people encounter risks in the digital world, just as in the offline world. However, these should be the exception and not the rule. As an effective regulator Ofcom need to ensure that the majority of children are protected for the majority of their time spent online. The popularity of VSPs among young people indicates the importance of enforcing robust regulation in this area.
Question 24: How should VSPs balance their users' rights to freedom of expression, and what metrics should they use to monitor this? What role do you see for a regulator?	Confidential? – N A focus on the design choices that put children at risk from harmful and illegal content, rather than taking down individual pieces of content, need not constrain or be conflated with users' rights to freedom of expression. As Cobbe and Singh[47] outline, algorithmic recommendation systems should be of regulatory focus as opposed to individual pieces of content. This is because intervention at this level does not infringe on an individual's freedom to post content in the first place, nor the current liability regime which affords online platforms immunity.[48] It is explained that, *'when it comes to systemic societal issues like disinformation, conspiracy theories, violent extremism, and political manipulation, content isn't by itself the problem. On its own, or viewed by only a small audience, a video promoting a conspiracy theory isn't a public policy issue. It becomes one when it has a large audience, and when it combines with other, related content that works to reinforce the message. Where content is algorithmically disseminated through recommending, this (a) increases its audience, potentially significantly, and (b) typically puts it alongside other, similar content. [...] Interventions focused on the hosting of content itself miss, to a large extent, issues relating to algorithmic dissemination.'* Algorithms are integral to the experience of the user but the basis on which they 'optimise' the user experience is opaque to anyone outside the company. Without algorithmic oversight it is

[47] Jennifer Cobbe and Jatinder Singh (2019) 'Regulating Recommending: Motivations, Considerations, and Principles', European Journal of Law and Technology, 10 (3)

[48] E-Commerce Directive – link to Arts 12-15

	increasingly impossible to ascertain the nature, presence or responsibility for harms experienced by young people. VSPs should have a duty to account for their algorithm. *Regulated services must:* • make their algorithms available for inspection and audit by the regulator, in order that the regulator can assess their compliance with the duty of care and published guidance; • assist the regulator in understanding the purpose and policies of the algorithm, identifying and assessing the data used to train the algorithm (and how it was collected), analysing the source code and/or statistical model in use, assessing the impact of the algorithm, and conducting its own tests on how the algorithm operates in practice and over time;[29] • have regard to any guidance on default settings produced by the Regulator; and • detail in their Child Impact Assessments the risks their algorithms pose to young people and what risk-mitigating action they have taken. In addition to external oversight of algorithms (that recommend content to children *and* recommend children's content to other users) as outlined in the points above, VSPs should be assessed against whether they are upholding their published terms. Child impact assessments would form a useful mechanism for the VSPs against which the regulator can judge the steps they have taken to mitigate risk on their service and, indeed, whether the measures they have deemed to be appropriate and proportionate are comprehensive enough. **What role do you see for the regulator?** • Enforcing/ supporting VSPs to conduct CIA as mandatory • Ensuring VSPs uphold their own published terms and sanctions when this is not the case. • Robust reporting mechanisms suitable for children.
Question 25: How should VSPs provide for an out of court redress mechanism for the impartial settlement of disputes between users and VSP providers? (see paragraph 2.32 and article 28(b)(7) in annex 5).	Confidential? – N In order to assist the Regulator in overseeing and enforcing compliance with the duty of care, a super-complaints regime should be established, allowing certain expert not-for-profit bodies to take representative action on behalf of users in the UK. Given the complexity of the digital world and the maturity of young people, it is not acceptable to

Please provide evidence or analysis to support your answer wherever possible, including consideration on how this requirement could be met in an effective and proportionate way.	require them to make individual complaints to seek redress for harm. Young people cannot be said to have meaningful access to justice when platforms routinely ignore complaints from users, even about content and conduct which violates their published terms and it would not be acceptable to expect that young people should go to court to enforce the duty of care.
Question 26: How might Ofcom best support VSPs to continue to innovate to keep users safe?	Confidential? – N Carrying out research with users will enable Ofcom to prioritise the aspects of innovation that will have the greatest impact on keeping users, including children safe. User insights and evidence from civil society should also inform the development of impact assessment tools that embed safety by design and privacy by design If Ofcom encourages VSPs to prioritise the best interests and safety of children by ensuring the assessment and mitigation of design level risks, this would not only aim to drive up standards of design but also prevent the need for retrofitting safety solutions that address narrow issues.
Question 27: How can Ofcom best support businesses to comply with the new requirements?	Confidential? – N Below are ways that Ofcom can support businesses to comply with the new requirements: • Provide clear guidance for innovators, including which services fall within scope. • 2.6 of Ofcom's call for evidence notes that some popular VSPs fall outside of the jurisdiction of the UK regulator I.e. YouTube, Facebook and Twitter. However, where content is viewable in the UK, then it should conform with UK rules. • VSPs should be incentivised to work within the regulation. Providing models and case studies of best practice and a range of tools (for example, robust 'off the shelf' options for age verification approved by the regulator and child impact assessment tools) would aid businesses. • Fees incurred for being regulated, as stated in 2.24 disincentivises VSPs from reporting to the regulator and indeed declaring that they are in scope. 2.24 requires revision and VSPs may be fined for not declaring if they fall in scope but should not have to pay to be regulated. • Clearly communicate to VSPs that that preventative action to mitigate risks to users, at the design stage, is in VSPs financial interests as opposed to retrofitting solutions. • Host sandbox sessions and support innovation building. • Foster dialogue across civil society and industry.

	• The regulator should allow, without prejudice, questions from VSPs as part of ongoing industry engagement. • Ensure incremental steps asking for changes before punitive measures such as fines are applied.
Question 28: Do you have any views on the set of principles set out in paragraph 2.49 (protection and assurance, freedom of expression, adaptability over time, transparency, robust enforcement, independence and proportionality), and balancing the tensions that may sometimes occur between them?	Confidential? – N Overall, the principles should ensure the prioritisation of young people's best interests and safety. Below we identify specific principles that could go further still to do so. The current principle for **protection and assurance** would benefit from defining some of the kinds of 'statutory protections' that VSP regulation plans to put in place ahead of Online Harms legislation. Ofcom has the opportunity to provide clear, practical steps that VSPs can take to ensure child safety is prioritised ahead of legislation. For example, protection and assurance should also include protections in the form of child impact assessments and proportionate and appropriate age verification. On **safeguarding freedom of expression**, Ofcom states that the regulator will provide guidance that sets 'clear expectations for regulated services to safeguard freedom of expression'. As discussed at length in response to question 24, the regulator should explicitly map out a focus on algorithmic recommendation systems and safety/privacy by design, as opposed to individual pieces of content. This is because intervention at this level does not infringe on an individual freedom to post content in the first place, nor the current liability regime which affords online platforms immunity. Providing clarity in this regard could also go some way to allay concerns about safeguarding and freedom of expression that can distract from the prioritisation of children's safety. Focusing on regulating at the level of system design of VSPs would also support principle 3, **adaptability over time**, as this enables new technologies to be built with children's best interests in mind, as opposed to retrofitting solutions or chasing individual pieces of content as the platforms, and how this content is experienced by users, changes over time. Whilst fully supporting the principle for **robust enforcement**, as discussed in detail in response to questions 20 and 21, given the vast popularity of VSPs among young people, the regulator should hold regulated services accountable when they allow children under the minimum age of usership identified in published terms to use the service. Robust enforcement must therefore include a recognition that regulated services must do more to verify the age of users (in a way that is proportionate and appropriate for the service) as a necessary step towards compliance.