Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material

Statement

Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material – Welsh overview

Contents

1. Overview

Draft guidance – in brief

Ofcom has been given new powers to regulate UK-established video-sharing platforms (VSPs). VSP regulation sets out to protect users of VSPs from specific types of harmful material in videos. This includes protecting under-18s from potentially harmful material and all users from material inciting violence or hatred, and content constituting criminal offences relating to terrorism; child sexual abuse material; and racism and xenophobia. VSPs are also required to ensure certain standards around advertising are met.

The statutory framework sets out a list of measures which providers must consider taking, as appropriate, to secure the required protections. These new requirements came into force on 1 November 2020.

Ofcom consulted on draft guidance for VSP providers on the regulatory requirements between 24 March 2021 and 2 June 2021. This covered the measures set out in the statutory framework and how these might be implemented. The draft guidance included, among other things, information on:

- Having, and enforcing, terms and conditions for harmful material

- Having, and effectively implementing, flagging and reporting mechanisms

- Applying appropriate age assurance measures to protect under-18s, including age verification for pornography.

The consultation document sets out additional information about the draft guidance, including the evidence we relied upon to support the guidance.

The purpose of our guidance is to help service providers understand:

a) the regulatory requirements under the VSP Framework which relate to the protection of users from harmful material;

b) what types of content might constitute harmful material in videos;

c) the measures platforms can take to protect users from that harmful material and guidance on how to implement those measures effectively;

d) the practicable and proportionate criteria providers must consider when deciding which measures to take;

e) how and why the use of additional steps to help protect users is encouraged, including implementing a risk management process; and

f) information about Ofcom's approach to monitoring and enforcement.

We received 28 responses in total, including 9 from service providers. We have carefully considered all responses in finalising our guidance and have published all non-confidential responses on our website. We received responses on a range of issues across the 16 questions raised by the draft guidance. We set these out in detail, and our conclusions, in Section 2 of this document.

We also discussed our guidance during the consultation period with service providers and other regulatory authorities. Where appropriate, we have reflected their comments in this statement and our final guidance.

We have published our final guidance alongside this statement.

Providers can email Ofcom at VSPRegulation@ofcom.org.uk if they have any questions about the final guidance or any other aspects of VSP regulation.

You can also read here about Ofcom's aims for the VSP Regime and the work we have planned for the year ahead in our Plan and Approach document.

2. Introduction

Background

2.1   Video-sharing platforms (VSPs) established in the UK are subject to new statutory regulations. VSP providers are required to take appropriate measures to protect under-18s from potentially harmful material and to protect the general public from incitement to hatred or violence and other specific material the inclusion of which would be a criminal offence. Services also need to ensure certain standards around advertising are met.[1] Ofcom is the independent communications regulator in the UK charged with overseeing this regulatory regime.

2.2   The statutory framework for the regulation of VSPs is set out in Part 4B of the Communications Act 2003 ("the Act"). Part 4B was introduced under regulations made by the Secretary of State to implement the revised Audiovisual Media Services Directive ("AVMSD" or "the Directive") and came into effect on 1 November 2020.[2] In this document we refer to the regulatory framework set out in Part 4B of the Act as "the VSP Framework" or "the VSP Regime".

2.3   The VSP Framework requires providers to take appropriate measures to protect users from harmful material in videos. A list of the measures providers must consider taking is set out in Schedule 15A of the Act. Ofcom is required to draw up and consult on guidance for providers of video-sharing platforms concerning the measures in Schedule 15A that may be appropriate for protecting users from the specified categories of harmful material, and the implementation of such measures. The measures are summarised as follows:

   a)   measures relating to terms and conditions

   b)   measures relating to the reporting, flagging or rating of content

   c)   access control measures such as age assurance and parental controls

   d)   complaints processes

   e)   media literacy tools and information.

2.4   To inform the development of guidance, Ofcom sought information from industry and other stakeholders through a call for evidence conducted in summer 2020 and commissioned new consumer and academic research. We produced a consultation document, which presented these findings, and, where relevant, other areas of consideration which we took into account in our draft guidance. A full version of the draft VSP guidance is available on the Ofcom website.

---

[1] The legislation refers to "audio-visual commercial communications" ("AVCCs"). AVCCs is a term applied across a number of sectors and includes advertising, as well as sponsorship, teleshopping and product placement, but also influencer marketing and other forms of commercial communication associated with VSPs. In this guidance, "adverts" and "advertising" are used as a short-hand for "AVCCs".

[2] Some aspects of the regime, such as the requirement to notify Ofcom and to pay a fee, come into force at later dates.

2.5   The regulation of UK-established video-sharing platforms is expected to be superseded by new legislation following the commencement of the online safety regulatory framework. In May 2021, the Government published its draft Online Safety Bill, confirming its intention to eventually repeal Part 4B of the Act. The online safety legislation will apply to a much wider range of online services, including services which are not established in the UK. Ofcom will operate the VSP Framework until such time as it is no longer in force and will ensure that there is support for services transitioning between the VSP and online safety frameworks.

Ofcom's approach to VSP regulation

2.6   **VSPs in scope are required to notify to Ofcom:** Service providers will need to consider whether the service they provide meets the scope and jurisdictional criteria set out in the Act. If it does, they are required to submit a formal notification of their service to Ofcom. Ofcom has published guidance to help providers assess whether their service is in scope and needs to be notified to us.[3] We have published a list of notified VSP providers on our website and will keep this updated as new services notify.[4]

2.7   **Services are required to take appropriate measures to protect users from harmful material:** The guidance is designed to help providers consider which of the measures listed in Schedule 15A of the Act it is appropriate to take, and how those measures might be implemented effectively. The guidance on protection measures is not prescriptive but intended to give suggestions to aid understanding of how users can be appropriately protected from harmful material. In some instances, there may be other ways to implement a measure to achieve the same purpose.[5] Where we think users are unlikely to be adequately protected without a specific approach, we say so in our guidance. We are recommending providers put in place systematic risk management processes to help providers to identify and implement measures that are practicable and proportionate and protect users. The guidance explains how this could be conducted.

2.8   **We will monitor and assess VSP providers' compliance with their regulatory obligations:** We will work closely with VSP providers to understand existing practices and the risks associated with their services. We will help providers understand what is expected of them and what more they need to do to tackle the risks identified. There are a number of sources of information we will draw on to monitor and assess providers' compliance, including: the exercise of our formal information gathering powers; reviewing trends in user complaints to Ofcom; informal engagement with the platforms; and regular engagement with tech safety groups, civil society organisations, and charities with an interest in online safety. We will also continue to be informed by our extensive programme of consumer research to gain insights into user experiences online and monitor trends.

---

[3] All notifications will need to be submitted via a dedicated web portal on Ofcom's website.
[4] The list of VSPs notified to Ofcom is available here: https://www.ofcom.org.uk/tv-radio-and-on-demand/information-for-industry/vsp-regulation/notified-video-sharing-platforms
[5] There may also be other measures not listed in the VSP Framework which may achieve the same protections.

2.9 **Flexibility and proportionality will underpin our approach:** The focus of the regulation is on making sure platforms take appropriate steps to protect their users from harmful material. The diversity of the VSP market means the risks they may pose, and the protections they need to offer to keep users safe, both vary. Consequently, Ofcom will not take a 'tick-box' approach to compliance. The onus will be on VSP providers to determine how best to manage the risks their services pose, and to take action that is proportionate to the risk of harm and tailored to the circumstances they face. We will take an evidence-based approach, targeting the greatest risks of harm and assessing the effectiveness of companies' chosen protective measures. We expect companies to be proactive, anticipating risks and taking proportionate preventative steps. This does not mean general monitoring for harmful content. It means platforms should regularly and systematically work to combat existing and emerging risks to ensure they protect their users effectively, using appropriate measures.

2.10 **We will take a holistic view of compliance:** We will take into account the steps providers have taken to identify and mitigate risks of harmful material and the overall efforts the platform has undertaken to provide appropriate protection measures for their users. Ofcom's understanding of which measures are appropriate and what constitutes effective protection for users will develop over time and we recognise that both platforms themselves and the risk of harm on those platforms will evolve.

2.11 **Robust enforcement where we see significant harm that is not being addressed:** Providers can expect a rigorous but fair approach to our new duties. We expect platforms to engage constructively and openly with Ofcom and be willing to make improvements where necessary. Although we have formal enforcement powers, we will generally seek to resolve issues with platforms before taking formal enforcement action. If Ofcom decides that formal enforcement action is necessary, we will investigate the issue to determine if there has been a breach and what further action may be appropriate. Where we record a breach, we have the power to issue sanctions under the VSP Framework which could include requiring the provider to take specific actions, imposing a financial penalty, and/or suspending or restricting the service.

2.12 **Safeguarding freedom of expression:** freedom of expression is a fundamental human right and we will always take it into account.[6] Companies themselves have no obligations in the VSP Regime to uphold freedom of expression, but Ofcom is legally bound to take into account these fundamental rights. Our guidance for VSP providers has been drafted in accordance with these rights.

---

[6] The right to freedom of expression exists at common law and in the Human Rights Act 1998, which incorporates the European Convention on Human Rights, including Article 10, into domestic law.

3. Consultation responses and Ofcom's conclusions

3.1   This Section summarises the key issues raised by respondents and Ofcom's response to them, including changes we have made to the final guidance document. The final guidance has been published alongside this statement on our website.

3.2   Our consultation document asked 16 questions, based broadly on the different Sections of the draft guidance. The questions we asked are copied in full below.

> **Question 1:** Do you have any comments on Section 3 of the draft guidance on harmful material and related definitions?
>
> **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?
>
> **Question 3:** Regarding terms and conditions which prohibit relevant harmful material, do 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?
>
> **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?
>
> **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?
>
> **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?
>
> **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 must have robust age verification in place?
>
> **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.
>
> **Question 9:** Do you have any comments on the draft guidance about parental control systems?

Question 10: Do you have any comments on the draft guidance about the measure regarding complaints processes or on the regulatory requirement to provide for an impartial dispute resolution procedure?

Question 11: Do you have any comments on the draft guidance about media literacy tools and information?

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?

Question 13: Do you have any comments on the draft guidance about assessing and managing risk?

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)?

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?

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

3.3   The questions above fall under the areas outlined below. This statement is structured according to these areas, taking each of the relevant issues raised by respondents in turn and setting out our response.

Theme	Question
Harmful material	Q1
Terms and conditions	Q2, Q3, Q4
Reporting and flagging	Q5
Ratings	Q6
Age assurance	Q7, Q8
Parental controls	Q9
Complaints	Q10
Dispute resolution	Q10
Media literacy	Q11
Practicable and proportionate	Q12
Risk management	Q13
Measuring effectiveness	-
Monitoring and enforcement	-

Impact assessment	Q14, Q15

Harmful material and guidance on statutory definitions

3.4   In our guidance, we set out that VSP providers should take appropriate measures to protect users from harmful material, noting that where a measure is taken, it must be implemented in such a way as to carry out the requirement to protect under-18s from restricted material and/or the general public from relevant harmful material (see paragraph 2.33). Our guidance on harmful material, including definitions of restricted material and relevant harmful material, is covered in Section 3 of the guidance

Restricted Material

3.5   In Section 3 of the draft guidance, we outlined the different types of material caught under the definition of 'restricted material'. The legislation does not specify any particular examples of material that "might impair the physical, mental or moral development of under-18s", so our guidance in this Section is designed to help providers understand what types of material they should consider here, and points to relevant research to aid that consideration.

What respondents said concerning Restricted Material

Definitions

3.6   Some respondents considered that the legislation was not sufficiently clear about what content 'might impair the moral, mental and physical development of minors', and several submissions asked for Ofcom to provide further guidance. **techUK** asked for more clarity on which harms are included in the regime and how, with examples and guidance. Others asked for any new category of harmful material to be defined clearly and precisely or it would otherwise lead platforms to take a risk-averse approach to enforcement and excessively censor legitimate content and infringe on freedom of expression.

3.7   Other respondents welcomed clearer guidance from Ofcom about what can be considered harmful. Some felt that the additional research commissioned on the protection of minors was quite extensive and that the guidance was sufficient.

3.8   **TikTok** welcomed Ofcom's acknowledgement that the implementation of measures will not necessarily achieve total eradication of harmful material from a platform. It also highlighted that their community guidelines went beyond the regulations, and that Ofcom should recognise the complexity and subjectivity in creating and implementing policies for content that may impair minors.

3.9   **ISBA** considered it essential to have a common framework of definitions for harmful content, such as the one created by the Global Alliance for Responsible Media.

Self-injurious content

3.10   **The Samaritans** welcome the inclusion of self-injurious content in guidance as an example of material that may impair under-18s and ask that it also includes: promotion or encouragement of self-harm and suicide; graphic descriptions or depictions of acts of self-harm and suicide, including descriptions and depictions of equipment; and the evaluation or comparison of the effectiveness of different methods, and suicide pacts and challenges, where users may be encouraged to harm themselves. The Samaritans refer to their industry guidelines for managing self-harm and suicide content and call for the guidance to advise services to have robust policies for self-harm and suicide material.

BBFC guidelines

3.11   There was some confusion about the role of BBFC certification, with some respondents incorrectly interpreting the regulations to mean that VSP definitions should be mapped with the BBFC's content ratings. The **Liberal Democrats DCMS Team** called for BBFC ratings to be a requirement in the VSP Regime, while others considered the ratings were not readily comparable to user-generated content and could therefore not be used. Other respondents considered that consulting BBFC guidelines unsuitable for classification required significant time and resources, impacting on the ability of online platforms to tackle harmful content.

3.12   **ISBA** asked for R18 categories of content to be exempt for their journalistic and educational value. The examples given referred to videos that condemn acts of violence, self-harm content uploaded by health bodies or NGOs supporting vulnerable individuals.

Other points raised

3.13   The **Liberal Democrats DCMS Team** and **techUK** called for the guidance to be kept under review to incorporate harms that might be included in the Online Safety Bill, such as societal harms. **TikTok** noted that VSP providers should not be required to comply with higher standards in the VSP Regime, given that the Online Safety Bill will introduce broader obligations to protect minors.

3.14   **TikTok** asked for Ofcom to be aligned with other regulatory frameworks, such as the Irish DPC's Fundamentals for Child-Oriented Approach to Data Processing, and the ICO's Age Appropriate Design Code requirement to establish age with a level of certainty that is appropriate to the risks.

3.15   The **Age Verification Providers Association (AVPA)** noted that the regulations were confusing, hindering a common understanding, consistency and a level playing field for services. AVPA also considered that while children of similar ages may not mature equally, what might impair the development of an average child today would remain relatively similar in future.

3.16   **5Rights Foundation** considered it important for services to take a holistic approach to protection of minors by considering design and functionalities that create risks for under-18s.

3.17   Regarding the definition of Restricted Material, this is a statutory definition and Ofcom does not have powers to change or amend this. However, we recognise that not all VSP providers will be familiar with content that may fall under this category and therefore have published academic research to help providers consider the kinds of material that might be present on their service.

3.18   Several respondents misunderstood the legal requirements of the VSP Regime and the role of Ofcom guidance, particularly in relation to BBFC classification and the definition of Restricted Material. Ofcom's references to the BBFC guidelines in Section 3 is a reflection that the legislation incorporates the BBFC's classifications for R18 and Prohibited Material into the definition of Restricted Material. It is important that platforms take the time to understand these definitions in full; however, platforms are not required to classify or require users to use BBFC content classifications.

3.19   Ofcom commissioned research from experts at the University of East London, to aid VSP providers in considering a range of factors that will inform how best to support under-18 users on their platform. This report helps platforms to consider a range of risks relevant to under-18s, including different types of self-injurious content.

3.20   We have not added further detail to the guidance about the interpretation of restricted material at this time. However, as we work with platforms over the first year of regulation, we will be considering what further information or advice providers might find useful to support the development of policies on restricted material. Ofcom and the ICO are also committed to working together to promote best practices in age assurance, compliant with both the privacy requirements in data protection law and the VSP Regime.

Relevant harmful material

3.21   Our draft guidance outlined the types of material caught under the definition of relevant harmful material, and the relevant pieces of legislation VSP providers need to be aware of.

3.22   Several respondents told us the draft guidance was too broad and vague around the definition of incitement to hatred. **The National Secular Society** called for more comprehensive explanations, in particular regarding religion or belief to ensure platforms do not disregard freedom of expression. **techUK** and **Tech Against Terrorism** called for more guidance and examples on what constitutes incitement to hatred. Tech Against Terrorism also said the lack of a practical framework on how to assess incitement to violence and hatred will make it harder for VSPs to correctly identify terrorist and violent extremist content, as the two often overlap. The **Board of Deputies of British Jews** suggested including 'national origin' as a protected characteristic to protect those attacked based on their Israeli national origin/nationality.

Ofcom response

3.23   Whether or not a video may incite violence or hatred is a fact-specific question that will depend on the particular context. Given this, prescriptive guidance in this area could never cover every possible form of incitement and so would risk being misleading.

3.24   However, in light of respondents' concerns, we have clarified the distinction between material likely to incite hatred and material likely to incite violence, and that providers need to ensure their policies take both forms of incitement into account. 'Hatred' refers to a feeling of animosity or rejection with regard to a person or a group of persons, aimed at one or more protected characteristics.[7]

3.25   With regard to how incitement to hatred on the basis of religion or belief should be understood and applied by platforms, Ofcom acknowledges that the boundaries between what may and may not be considered legitimate debate when assessing whether content constitutes incitement to religious hatred can be hard to define. (Ofcom commissioned research from experts at the Alan Turing Institute which VSP providers may find useful for understanding online hate.) We recognise that providers may have to make nuanced and difficult judgments at times on where the line falls between robust criticism of a religion and incitement to hatred of its adherents, and do not consider this can be avoided. It is not a requirement of the VSP Regime that providers will always accurately assess whether material is likely to incite violence or hatred. When considering the appropriateness of platforms' measures, we will have due regard to how difficult these judgments can sometimes be to make.

3.26   We accept incitement to violence and hatred on the basis of national origin is within the scope of the listed protected characteristics. It could be considered to fall under a number of the grounds, in particular 'ethnic origin'. We note, in addition, that the definition of relevant harmful material expressly includes content caught by Article 1 of Council Framework Decision (2008/913/JHA) of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. This includes publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to national origin.

What respondents said about the guidance for material concerning terrorism, racism, and xenophobia

3.27   As set out above, **Tech Against Terrorism** said the 'lack of a practical framework on how to assess incitement to hatred and violence will also complicate platforms' capacity to correctly identify terrorist and violent extremist content, as the two types of content often overlap in practice.' They recommend Ofcom provide lists and definitions of proscribed content and behaviours based on the rule of law by 'clearly referring to existing law on

---

[7] As noted in Section 3 of the guidance, the definition of Relevant Harmful Material includes incitement to violence or hatred against a group of persons, or a member of a group of persons, based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

counterterrorism and acceptable limits to freedom of expression which lay out what is considered illegal speech'. They said the guidance should be based on the rule of law derived from international standards. Tech against Terrorism also recommended that Ofcom develop the guidance to include practical guidelines for providers regarding what form prohibitions of harmful content should take. **National Secular Society** and another respondent also said that platforms require more clarity about what constitutes illegal material.

3.28 One VSP provider also asked for guidance on harms definitions to be the same or applicable in other countries.

3.29 One platform said deciding what is illegal risks being unduly onerous, particularly for small platforms, and could result in over-removal. Similarly, **TikTok** warned that incorporating elements from criminal offences, such as 'intent', into scalable moderation systems would be challenging and would lead to over-removal, thus undermining the freedom of expression of users.

3.30 One respondent said that reference should be made to denial, distortion and trivialisation of the Holocaust as a particular example of a widespread and pernicious type of genocide denial.

Ofcom response

3.31 We note respondents' concerns relating to the lack of a practical framework around incitement to hatred complicating providers' efforts to identify criminal terrorist content. We have therefore added to the guidance to provide suggestions for providers regarding good practice for terms and conditions prohibiting incitement to hatred or violence (see page 26 of the guidance).

3.32 Ofcom is committed to interpreting and applying the VSP Framework in compatibility with the Human Rights Act 1998 and the European Convention on Human Rights, under which freedom of expression is a fundamental right.[8] Our guidance for VSP providers has been drafted in accordance with these rights.

3.33 We acknowledge the calls of several respondents for clearer guidance for providers regarding what constitutes illegal material. We recognise that implementing the legislation may involve nuanced interpretation of what constitutes illegal material but providers will need to seek their own legal advice, as appropriate. We have however indicated that terms and conditions relating to terrorist, racist and xenophobic content should not be defined any more narrowly than criminal offences set out in the Act. In paragraphs 7.16 to 7.25 of the guidance we suggest a number of third-party organisations who can provide expert advice to providers regarding illegal material and the drafting of terms and conditions.

3.34 In response to the request that guidance on harms definitions should be the same or should also be applicable in other countries, it is not within Ofcom's gift to dictate the

---

[8] The right to freedom of expression exists at common law and in the Human Rights Act 1998, which incorporates the European Convention on Human Rights, including Article 10, into domestic law.

guidance offered by other regulators. However, the UK's VSP Regime originates from an EU Directive, which aims to ensure consistency across member states. Ofcom will continue our close working with international regulators to share learning and understand their approaches to VSP, and wider online, regulation. We will aim to align approaches where we consider that this will deliver the greatest protection for UK users and promote compliance across industry.

3.35   In relation to the suggestion of practical guidance that may prove useful to providers, we will consider whether it is appropriate to publish further information or guidance on particular topics.

3.36   We also recognise that the Holocaust is a clear example of genocide and thus would fall within the scope of 'genocide denial'.

What respondents said about the guidance concerning Child Sexual Abuse Material (CSAM)

3.37   Several respondents, including the **NCA**, noted the use of the term 'child pornography' and requested that this was amended to CSAM.

3.38   Automatic scanning of content upon upload to check whether content contained CSAM was recommended by the **NCA.**

3.39   The **NSPCC** noted that there should be greater emphasis on the circumstances under which CSAM is produced. In particular, the NSPCC highlighted the role that grooming might play in the production of youth-produced sexual imagery.

3.40   The **NSPCC** also expressed concern that online sexual grooming was included within a list of harms that also included legal content (such as pornography), which did not properly highlight that the gravity of grooming, which is also a criminal offence.

Ofcom's response

3.41   Ofcom acknowledges that the phrase 'child pornography' is considered problematic and is not in common use across the UK. However, the guidance needs to reflect the specific wording within the legislation. Its use has therefore been limited, where possible, within the guidance.

3.42   The use of automatic scanning technology to prevent the upload of CSAM is becoming more commonplace within industry. Ofcom understands this can provide added protection for users. However, such technology would be considered to be proactive monitoring, which the legislation does not require platforms to undertake.

3.43   We recognise the **NSPCC's** comments regarding the role that online grooming can play in the production of new CSAM. However, this falls beyond the scope of the current VSP Regime. Ofcom also acknowledges that grooming is an illegal activity that should be considered as distinct from legal content such as pornography. The guidance has been amended to reflect this legal distinction.

3.44   Ofcom also recognises the potential risks involved in a crowd-sourcing approach to moderation, particularly to decide whether content is CSAM. Therefore, this has also been included within the guidance.

Protection measures

Terms and conditions

3.45   In our draft guidance (see paragraphs 4.15 to 4.53), we said that terms and conditions should explain the type of content considered to be restricted material and specify that videos containing this material must be brought to the attention of the VSP provider. We said we were of the view that terms and conditions were unlikely to secure effective protection of under-18s unless viewers are also notified where a video contains restricted material or access to it by under-18s is restricted.

3.46   Regarding terms and conditions prohibiting users from uploading videos containing relevant harmful material, we said that Ofcom considers this measure to be fundamental to the VSP Regime and that we consider it unlikely that effective protection of users can be achieved without having this measure in place and it being implemented effectively.

3.47   In our draft guidance, we said that VSP providers should have regard to the length; readability; location; format; timing and promotion of terms and conditions to ensure they are effective and easy to use. We said that platforms with a typically younger user profile should consider providing child-friendly explanations. We also said that VSP providers should consider how frequently users should be prompted to engage with terms and conditions based on a platform's own risk profile.

3.48   Regarding the effective implementation of terms and conditions, we said this will likely mean having robust processes in place to ensure terms and conditions are appropriately enforced. We said that violations of the terms and conditions should result in effective action being taken by the VSP provider and that Ofcom expects any moderation techniques used (whether human or technological) to be subject to regular quality assurance processes. We encouraged VSP providers to collect information to assess the effectiveness of any moderation techniques used.

3.49   We said that, in the interest of transparency, the consequences of breaching terms and conditions need to be clear to all users. We also said that providers should ensure that terms and conditions are enforced in a manner that does not unduly discriminate between users and that where sanctions are applied, users need to have the ability to understand and challenge these decisions.

3.50   In the draft guidance, we said that we expect VSP providers to keep terms and conditions under review and make changes where necessary. We said that VSP providers should also be aware of potential changes to the ways in which users interact with their platform as these might change the risk profile of the platform and terms and conditions may need to adapt to reflect this.

What respondents said about the guidance on terms and conditions in general

3.51   Several respondents supported Ofcom's draft guidance on terms and conditions. They agreed that terms and conditions are fundamental to the VSP Regime and need to be enforced consistently and transparently.

3.52   **National Secular Society** agreed with our guidance that providers should ensure they remain informed about changing societal attitudes, as what constitutes 'restricted material' is likely to change over time.

3.53   One VSP provider said that drafting terms and conditions would be costly for smaller VSP providers without in-house legal resource.

3.54   Other respondents made suggestions about how to improve the draft guidance, including: making VSP providers comply with stricter terms and conditions (**Board of Deputies of British Jews**); ensuring VSP providers make regular commitments to uphold their terms and conditions; tailoring terms and conditions to the needs of different demographics (**Tech Against Terrorism**); and emphasising that VSP providers should take a holistic view to protecting under-18s (**5Rights Foundation**).

3.55   Several platforms provided examples of the terms and conditions they have in place to protect users and details of their moderation and enforcement strategies. **Tech Against Terrorism** provided details of its work to help VSP providers protect users on their platforms and **SWGfL** provided examples of their work to protect users online. **ISBA** provided details of the framework adopted by the advertising industry for defining content inappropriate for advertising.

Ofcom's response

3.56   We acknowledge one provider's concerns about the cost of drafting terms and conditions. However, we consider that having terms and conditions is a fundamental part of protecting users from harmful material. While resources (and therefore costs) are a consideration under the practicable and proportionate criteria, lack of resources alone will not be sufficient justification for not taking a protection measure that Ofcom considers to be appropriate in relation to a service (see paragraph 6.14 of the guidance).

3.57   We note the suggestions made by several respondents about how to improve the guidance, however, Ofcom is unable to require providers to go beyond the measures set out in the legislation. In the guidance we state that terms and conditions need to be implemented in such a way to meet the requirement of protecting users (see paragraph 4.41). We consider that it is more appropriate to ensure terms and conditions are upheld and enforced effectively in practice than to encourage providers to make regular public commitments to uphold them.

3.58   Regarding **Tech Against Terrorism's** response, in the guidance we state that providers should have regard to the profile of their users when determining which measures are appropriate (see paragraph 4.2). In the guidance we also state that providers are encouraged to take a safety-first approach and design their services with this in mind,

considering the needs of users in all decisions in order to develop a culture of safety (see paragraph 7.5).

What respondents said about terms and conditions about restricted material

3.59   Several respondents agreed 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. Other respondents agreed that the requirement to notify alone was unlikely to be effective at protecting users and welcomed the flexibility of Ofcom's approach.

3.60   **ISBA** said that a common framework of definitions of restricted material is essential but will be ineffective unless providers inform users of videos containing restricted material. They suggested that the responsibility should lie with providers to introduce controls asking users to notify the provider of what type of material they are uploading.

3.61   **SWGfL** noted that the need to take additional steps once notified in order to protect under-18s might discourage providers from introducing this measure.

3.62   **Fanzworld** said 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 only when relevant terms and conditions are not already in place. **TikTok** noted that this measure may not have a significant impact on some providers who already prohibit such content on their platforms. TikTok also raised concerns about users' accuracy when assessing their own content, given the subjective nature of restricted material.

3.63   The **NSPCC** said that an age-gate that children can choose to click through to access content is unlikely to offer substantive protections in practice but agreed that this measure could be effective if accompanied by age verification measures. They recommended that VSP providers should audit the extent to which users comply with the requirement to notify them of restricted material and set out what action will be taken against users who persistently fail to comply with this requirement. They suggested that providers should rely upon this measure only where it is cost-prohibitive or technically infeasible to deliver other more accurate and reliable solutions.

3.64   One VSP provider noted that this measure could be costly for VSP providers depending on the number of uploaders and the extent to which processes can be automated. They said they would welcome further guidance on how this measure might apply to sites that employ age assurance and verification systems to prevent under-18s accessing the site.

Ofcom's response

3.65   We acknowledge **ISBA**'s response as set out above and also note **TikTok**'s concern about users' accuracy when assessing whether their content contains restricted material. In light of these concerns we have added to the guidance to suggest that providers could consider introducing a step into the upload process to prompt users to consider whether they need to notify the platform of restricted material. This prompt could include information to help

users assess their content correctly, for example, an explanation of what constitutes restricted material or a reminder of the platform's terms and conditions, including potential sanctions (see paragraph 4.19).

3.66   Regarding the comments made by **Fanzworld** and **TikTok** about providers who prohibit restricted material on their platforms, we have clarified in the guidance that where there is material permitted on a VSP that may not be age-appropriate for all users of the platform, the provider should consider how the implementation of this measure can provide an age-appropriate experience for different age groups of under-18s. In the guidance we also recognise that this measure will not be necessary or appropriate for some types of platform, for instance, platforms specialising in restricted material of a pornographic nature. In such cases we expect providers to consider taking other measures to protect under-18s, such as having appropriately robust age-assurance systems in place (see paragraphs 4.22 to 4.23).

3.67   We note the concerns raised by the **NSPCC** regarding the controls used to protect under-18s from restricted material. We have added to the guidance that we encourage providers to assess how effectively they have implemented their terms and conditions and to consider setting out all potential sanctions in their terms and conditions (see paragraphs 4.42 to 4.51). We also state in the guidance that VSP providers must apply the principle that restricted material that has the most potential to harm under-18s must be subject to the strictest control measures (see paragraph 3.14).

3.68   We acknowledge one respondent's concern about the cost of this measure for providers. However, we consider that cost and resources cannot be considered in isolation when determining whether a measure is practicable and proportionate and that lack of resources alone will not be sufficient justification for not taking a measure that is appropriate for the purpose of protecting under-18s from restricted material (see paragraph 6.14 of the guidance).

What respondents said about terms and conditions about relevant harmful material

3.69   Several respondents agreed that prohibiting relevant harmful material is fundamental to the VSP Regime and that it is unlikely that effective protection of users can be achieved without having this measure in place and it being implemented effectively.

3.70   **SWGfL** noted that this measure is only effective if terms and conditions can be understood by users. **5Rights Foundation** likewise noted that effective protection will not be possible without regulatory oversight and enforcement.

3.71   The **National Crime Agency (NCA)** suggested that terms and conditions should explicitly set out the material that cannot be posted on the platform. They also said that it would be helpful for VSP providers' terms and conditions to set out explicit provisions for sharing information with police to prevent and/or detect crime.

3.72   The **NSPCC** recommended that the guidance clearly state that VSP providers should permanently remove and delete accounts that share child sexual abuse material and report any illegal activity relating to child abuse to law enforcement. They suggested that services

should be required to demonstrate that they have processes in place to proactively detect child abuse. The **NCA** also suggested that platforms should be pre-screening uploads to detect CSAM. **ISBA** and one civil society organisation likewise suggested that VSP providers should proactively monitor content on their platforms.

3.73   **ISBA** suggested that the guidance should mandate that content classed as relevant harmful material should not be monetised.

Ofcom's response

3.74   We note the suggestions made by the **NCA** and have added to the guidance to encourage providers to consider setting out all prohibited material clearly in their terms and conditions (see paragraph 4.51). Sharing information with law enforcement is a matter for individual VSP providers. However, we understand providers may wish to do so under certain circumstances, for instance, where they become aware of CSAM.

3.75   We acknowledge the suggestion made by the **NSPCC** above and have added to the guidance to encourage providers to ensure that their terms and conditions are clear about how they will deal with illegal content reported to the platform (see paragraph 4.27). We also state that we encourage providers to set out all potential sanctions in their terms and conditions (see paragraph 4.51 of the guidance).

3.76   We note the calls from several respondents for proactive monitoring and/or moderation of content. As noted in paragraph 3.42 above, the VSP Framework does not require platforms to proactively monitor or moderate content. However, we expect companies to demonstrate proactive risk management on their platforms and to assess the effectiveness of their protection measures on an ongoing basis (see paragraphs 7.26 to 7.49 of the guidance).

3.77   Regarding the suggestion made by **ISBA** above, we do not consider it appropriate to suggest that relevant harmful material should not be monetised, as under the VSP Regime providers need to take measures which prohibit this material from being uploaded to their platforms (see paragraphs 4.24 to 4.27 of the guidance). Where providers become aware of relevant harmful material, we would expect them to enforce that prohibition by removing the content in question.

What respondents said about ensuring terms and conditions are easy to use

3.78   **SWGfL** and **5Rights Foundation** agreed with the recommendation that platforms with large numbers of younger users should consider child-friendly terms and conditions. The **NCA** welcomed the guidance on ensuring terms and conditions are easy to use and can be understood by children and those whose grasp of the English language is not strong. **Tech Against Terrorism** said that the inclusion of guidance regarding the length and readability of terms and conditions is commendable.

3.79   **ISBA** and one civil society organisation said they supported the guidance that VSP providers should remind users of terms and conditions when they upload content.

3.80   **5Rights Foundation** and **ISBA** supported the five principles of implementation (effective, easy to use, transparent, fair and evolving). 5Rights Foundation recommended the guidance should stress that clear presentation of terms and conditions alone does not equate to effective implementation.

3.81   **SWGfL** highlighted its work on the use of 'labels' to make terms and conditions more accessible. They also suggested that VSP providers should have to provide evidence that users have understood the terms and conditions, rather than just accepting them, when registering for a service.

3.82   The **NSPCC** recommended that it should be made clear in platforms' terms and conditions that children can request the removal of distressing content.

3.83   Two VSP providers noted that terms and conditions cannot be so simplified that they are not fit to be a legal agreement. Another online service provider made a similar point, that balance is needed between brevity and simplicity on the one hand, and thorough coverage of all prohibited content and behaviour on the other.

3.84   One online service provider suggested that Ofcom could provide more guidance for VSP providers by providing examples, preferably visual, of good and bad practice. **techUK** recommended that Ofcom provide clearer guidance on what design changes or updates will be needed. They noted that the guidance will need to allow for diverse approaches due to the variation between different services.

3.85   Another VSP provider highlighted that repeated prompts to engage with terms and conditions could have an impact on the user experience.

Ofcom's response

3.86   We acknowledge **5Rights Foundation**'s concern regarding the effective implementation of terms and conditions. In paragraph 4.41 of the guidance we state that, in practice, effective implementation of terms and conditions means having robust processes in place to ensure terms and conditions are appropriately enforced. We consider this makes clear to providers that clear presentation of terms and conditions alone does not equate to effective implementation.

3.87   We note **SWGfL**'s suggestion that providers could use 'labels' to make terms and conditions easier to understand. In the guidance we highlight a study by the Behavioural Insights Team (BIT) which found that using summary bullet-points with icons illustrating key terms can lead to increased understanding of terms and conditions (see paragraph 4.31).[9] We have also added to the guidance to suggest that providers could consider evaluating users' engagement with and/or understanding of terms and conditions when assessing how effectively they have been implemented (see paragraph 4.42).

3.88   We welcome the **NSPCC**'s suggestion that terms and conditions should make clear to children that they can request the removal of distressing content. We have added to the

---

[9] Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses, The Behavioural Insights Team.

guidance to suggest that platforms may wish to consider whether there are specific aspects of their terms and conditions which it is particularly important for younger users to understand, for instance users' ability to report or flag content, and to consider tailoring their reporting and flagging processes to children (see paragraphs 4.32 and 4.68).

3.89   We note the concerns of several respondents regarding the need for a balance between simplicity and thoroughness when drafting terms and conditions However, we consider that it is nonetheless possible to draft legally binding terms and conditions that may be easily understood by users, or to provide an additional, more user-friendly version of terms and conditions, alongside the full legal document (see paragraph 4.34 of the guidance).

3.90   We acknowledge the calls for more guidance for providers regarding the presentation of terms and conditions. We consider that providers are best placed to judge how to tailor their terms and conditions to the needs of their userbase and agree with **techUK** that diverse approaches will be necessary given the variation between different services. We have added to the guidance that third-party organisations can provide resources and advice on how to draft user-friendly terms and conditions, for example, the Children's Commissioner's 'Growing up digital' report and BIT's 'Best practice guide' (see paragraph 4.34 of the guidance).

3.91   We note one VSP provider's concerns regarding the impact of repeated prompts to engage with terms and conditions on the user experience and recognise that this approach will not be appropriate for all platforms. It is for individual platforms to decide how best to implement their terms and conditions. However, we suggest that some providers might find it helpful to consider this suggestion as one way they could do so.

What respondents said about ensuring terms and conditions are effective

3.92   Several respondents agreed that terms and conditions need to be implemented effectively and that in practice this means having robust processes in place to ensure they are enforced and appropriate sanctions applied. **5Rights Foundation** particularly welcomed the recommendation that the accuracy of machine-learning moderation techniques should be checked by human quality assurance processes. **techUK** said that they support Ofcom's approach to enabling users to report content.

3.93   One VSP provider said they think it is important for consideration to be given to start-ups and "young" companies whose moderation teams may be trying to keep up with rapid expansion. They said they would welcome guidance about how information on the effectiveness of moderation methods can be collected. They noted that collecting this information could be a large task.

3.94   **Tech Against Terrorism** was concerned that the guidance does not provide enough detail on how to implement the measures in practice. They recommended that Ofcom provide detailed guides on different enforcement strategies. The **NSPCC** recommended that the guidance state more explicitly what moderation and enforcement processes will be considered necessary for a VSP to demonstrate compliance.

3.95   **5Rights Foundation** recommended that in addition to clear presentation, published terms and conditions should be supported by swift and easy access to expert advice and redress, preventing automated recommendation of harmful material, disabling of features that connect children with unknown adults, restricting design features that extend use (particularly auto-play or timed notifications), positive nudges to encourage time off, and ensuring informed consent (for example by providing transparency about the risks associated with the service).

3.96   The **Board of Deputies of British Jews** and the **NSPCC** were concerned that some VSP providers do not have adequate arrangements in place to enforce their terms and conditions and deter prohibited behaviour. The Board of Deputies of British Jews also stressed the importance of having UK-based moderation teams to ensure that moderators consider political, cultural and linguistic context when assessing content.

3.97   **Antisemitism Policy Trust** recommended that VSP providers should limit the degree of user anonymity. They suggested that platforms should adopt a "know your client" principle and revoke users' online anonymity if they violate the platform's terms and conditions.

Ofcom's response

3.98   We acknowledge one VSP provider's concern about "young" companies whose moderation processes may struggle to keep pace with their rapid expansion. When considering whether a platform has implemented protection measures effectively, we will consider the practicable and proportionate criteria set out in Section 6 of the guidance, including the size and nature of the VSP in question. With regard to the call for more guidance on how to collect information about the effectiveness of moderation methods, paragraphs 7.50 to 7.56 of the guidance provide more detail for providers about measuring the effectiveness of protection measures.

3.99   We note **Tech Against Terrorism**'s and the **NSPCC**'s responses as summarised above. The supervisory workstreams of our plan of work for the next 12 months will look at, among other things, practices related to platforms' terms and conditions, including their implementation.

3.100   We acknowledge **5Rights Foundation**'s recommendations to promote the safety of children online. In paragraphs 4.157 to 4.169 of the guidance, 'Media literacy tools and information', we set out guidance for providers about how they should consider using media literacy tools to help users of all ages use video-sharing platforms safely. In paragraphs 7.5-7.10 of the guidance, 'Embedding a safety-first approach', we also encourage VSP providers to take a safety-first approach to designing their service. However, we consider individual providers best placed to decide how to protect under-18s on their platforms.

3.101   We note the concerns raised by the **Board of Deputies of British Jews** and the **NSPCC**. In the guidance we state that terms and conditions need to be appropriately enforced by the provider and that serious violations and repeat offences should attract the toughest sanctions (see paragraphs 4.43 to 4.44). Should we have concerns that a VSP does not have

adequate processes in place to uphold and enforce their terms and conditions, and may therefore not have implemented the measures effectively, Ofcom would consider the appropriate course of action, including potential enforcement action.

3.102   Regarding the **Board of Deputies of British Jews**' recommendation that moderation teams be UK-based, it is for individual VSP providers to decide how best to moderate content and where to locate their staff. However, we consider that in many cases it will important for moderators to understand the political, cultural and linguistic context of the content they are assessing.

3.103   We note the suggestions made by the **Antisemitism Policy Trust**. However, as we state in the guidance, it is for individual providers to decide what action may be appropriate for particular violations and the thresholds for taking action (see paragraph 4.44).

What respondents said about ensuring the implementation of terms and conditions is fair and transparent

3.104   One online service provider was concerned about transparency when enforcing terms and conditions, arguing that it should be subject to limits to ensure it is proportionate. They warned that providing too much information to users risks enabling them to game the system and avoid moderation. They recommended that Ofcom distinguish between transparency data published for the general public and data provided to authorities for enforcement purposes. It noted that some data could be commercially sensitive.

Ofcom's response

3.105   In the guidance we state that providers should have regard to the practicable and proportionate criteria in Section 6 alongside the guidance on terms and conditions. With these criteria in mind, it is for individual platforms to decide what level of transparency is appropriate for their service. In the guidance we also acknowledge that it is often essential for moderation techniques to remain confidential to better allow VSP providers to effectively remove harmful material (see paragraph 4.51). Platforms may wish to consider this when deciding how much information about moderation and enforcement it is appropriate to disclose. Under the VSP Framework, it is likewise at the discretion of individual providers to decide what data they wish to make public in the interests of transparency (see paragraphs 7.50 to 7.56, 'Assessing effectiveness of protection measures', for more information on transparency reporting).

What respondents said about ensuring terms and conditions continually evolve

3.106   **Tech Against Terrorism** supported the recommendation that providers regularly review their terms and conditions. They recommended setting out specific factors VSP providers should consider when reviewing the terms and conditions. **SWGfL** agreed that providers should notify users of changes to terms and conditions.

3.107   We noted **Tech Against Terrorism**'s suggestion and have added to the guidance that examples of potential triggers for a further review of terms and conditions (in addition to regular, ongoing reviews) could include technological developments, new research or changes to the online environment, to platform features or to relevant legislation.

Reporting and flagging mechanisms

3.108   In our draft guidance (see paragraphs 4.54 to 4.72) we stated that VSP providers should establish and operate:

a)   transparent and user-friendly mechanisms for viewers to report or flag harmful material which is available on the service to the person providing the service; and

b)   systems through which the person providing the service explains to the persons using the service what effect has been given to the reporting and flagging referred to in sub-paragraph (a).

3.109   The draft guidance also stated that Ofcom considers reporting and flagging mechanisms fundamental to the protection of users and, as such, these mechanisms should be easy to use. In addition, actions taken in response to reports or flags should be clear, transparent, appropriately timely and proportionate to the size, nature and risk profile of the platform. Reports and flags should also be categorised and recorded (see paragraphs 4.58 to 4.72 of the guidance).

What respondents said about the need to establish reporting and flagging mechanisms

3.110   In general, respondents (including **Fanzworld, Liberal Democrat DCMS Team, NSPCC, Samaritans, SWGfL, Tech Against Terrorism,** and **TikTok)** agreed that reporting and flagging mechanisms are crucial for protecting users. **Vimeo** appreciated Ofcom's approach in allowing flexibility.

3.111   One respondent agreed that reporting and flagging tools are key and may work on mainstream VSPs; however, they said that these mechanisms need to be accompanied by proactive moderation measures by the provider themselves, as it is unlikely that users of fringe or extremist platforms will flag harmful content.

3.112   **Tech Against Terrorism** highlighted the importance of reporting and flagging mechanisms particularly for smaller platforms who lack the resources for proactive monitoring.

3.113   **techUK** highlighted a potentially adverse outcome of the proposed approach to reporting and flagging. Specifically, they referred to the fact VSP providers may need to provide users and non-users with details of what the potential outcome of their complaint is, but that users will complain about various topics and each of these will have specific priorities.

3.114   The **BBC** welcomed Ofcom's position that we would generally not expect content broadcast by regulated broadcasters to raise issues under the VSP Regime if already compliant with the Broadcasting Code. They suggested that special consideration should

apply to Public Service Broadcasting (PSB) content when flagged for removal. They also recommended that there be an expedited process for PSBs to report the misuse of PSB branding to platforms.

Ofcom's response

3.115   Ofcom acknowledges the consensus from respondents that reporting and flagging mechanisms are fundamental to the protection of users. While we note the calls for proactive monitoring measures to be implemented alongside reporting and flagging, the legislation does not require platforms to proactively monitor or moderate content. However, we recognise that some platforms do employ technologies that proactively monitor for harmful content; this remains at their discretion.

3.116   We acknowledge the **BBC**'s suggestions regarding the treatment of PSB content on VSP platforms. However, Ofcom is unable to require providers to give special consideration to PSB content or branding, and any change to the VSP Framework to enable this is a matter for Government and Parliament.

What respondents said about the ease of using reporting and flagging mechanisms

3.117   A number of respondents (**5Rights Foundation, Samaritans, NSPCC**) highlighted their concerns about young people reporting harmful material. **5Rights Foundation** said it should not be expected that a child will be able to identify or report content and that children find community guidelines confusing. They further explained that children may be hesitant to report content if they: think they may get into trouble; are worried that their device may be taken away; or do not trust that the system will take care of them.

3.118   **5Rights Foundation** said that relying on user reporting requires a child to understand the harm and their rights to be treated differently. They said that while swift, effective reporting is an important provision for children, it is not the 'central' mechanism for protecting users.

3.119   The **Samaritans** said that, based on research they did with young users, the term 'flagging' is preferred to 'reporting' as 'reporting' can be a deterrent. They also said it is important for mechanisms to be considered from the perspective of the user *and* the uploader, as the uploader may be vulnerable or distressed or in need of support.

3.120   The **NSPCC** also highlighted significant barriers associated with children feeling confident and willing to use reporting functions. **NSPCC** research found that:

- a significant proportion of young people aged between 13 and 17 do not know how to make reports on VSPs;
- less than three-fifths of young people know how to make a report on three major VSPs (**Snapchat, TikTok and Twitch**); and
- less than 5% of children aged 13-17 recall having made a report on these three VSPs.

3.121   **Tech Against Terrorism** and **SWGfL** both said that non-users and viewers without an account or who are not signed in should also be able to report/flag harmful material.

3.122   Concerns were raised about users feeling safe to report or flag content. One online service provider said reporting is nuanced and users who do not feel safe, can feel reluctant to report issues like abusive behaviour. **Fanzworld** suggested there should be confidentiality in reporting.

Ofcom's response

3.123   Ofcom acknowledges respondents' views in relation to children reporting harmful material, including confidence in using reporting systems and understanding how to flag content. We have strengthened the guidance to highlight that providers whose services have a high number of under-18 users should ensure that their reporting and flagging mechanisms are designed so they can be easily used by children (see paragraph 4.68 of the guidance).

3.124   In addition, we note concerns around some users not feeling safe to report. Providers should consider how they can work with experts and specialist charities to support users feeling safe (see Section 7 of the guidance).

3.125   In relation to the point the **Samaritans** made about uploaders of harmful content potentially being vulnerable or in need of support, we have strengthened our guidance on this (see paragraph 7.16). We have suggested that platforms could point users to resources created by experts (such as charities), including users who have been found to have uploaded harmful material.

3.126   In addition, our guidance also refers to the COM-B model (see paragraph 4.167) which is a framework that can help identify the barriers that different user groups might face. The guidance around this has been updated to highlight that different age groups within children will likely face different barriers (see paragraph 4.166 in the guidance).

3.127   With regard to users being able to report or flag harmful material without an account or without being signed in, Ofcom considers that reporting and flagging mechanisms should be available to anyone able to view content on a platform, and not limited to those logged in via an account. We have reflected this in our guidance (see paragraph 4.66).

What respondents said about actions taken in response to reports and flags being clear, transparent and appropriately timely

3.128   **SWGfL** agreed with Ofcom's research that users think flagging and reporting processes lack transparency, and evidence from their own research supports this. The **Samaritans** emphasised that information about reporting should be clearly accessible and displayed before registration. They also said that users should be regularly reminded of the reporting and flagging mechanisms, and any changes should be transparently communicated.

3.129   The **National Crime Agency (NCA)** said it would be helpful for the guidance to be specific that VSP providers should not flag illegal content to the user who has uploaded the video as this may alert them to the interest of law enforcement and potentially destroy evidence. They said that transparency of reporting and flagging is essential but should retain protections for the reporter and for law enforcement as necessary.

3.130   There were some concerns raised about responding to reports and providing an explanation of a report. One VSP provider supported the idea of responding to reports but queried whether providing an explanation is proportionate, as it would increase the burden on platforms and requires additional resources that not all VSPs have. This respondent also suggested a dedicated policy page that sets out likely actions instead. Another VSP provider said that a feedback loop is less desirable from a user experience perspective for their own platform.

3.131   The **NSPCC** said that the guidance does not go far enough in setting out clear expectations to VSP providers about how, and in what form, users should be informed or updated about decisions taken. They said improved decision notifications are likely to be the key driver of improved user engagement and confidence. Additionally, the **Liberal Democrat DCMS team** stated they think that the encouragement for providers to actively inform users about the process as they engage with it should be strengthened. **Tech Against Terrorism** suggested the guidance should recommend that platforms should notify users when their content or account is removed or actioned and to explain the moderation decision in full.

3.132   **Antisemitism Policy Trust** recommended that Ofcom defines what constitutes a timely response to reports or flags. They said that 'appropriately timely' is vague and difficult to enforce. They note that other European requirements are more onerous e.g. to require 'expeditious' removal of content.

3.133   The **NSPCC** welcomed the requirement of timely responses and that platforms should prioritise the most harmful content including child abuse. The **NCA** suggest that the speed from the report to when material is no longer available to users should be included in the effectiveness measures.

Ofcom's response

3.134   We acknowledge the views of the respondents. In the guidance we state that actions a platform will take in response to a flag should be apparent to all users, even those who have not yet engaged with the functionality (see paragraph 4.70). We also encourage VSP providers to actively inform users about the process as they engage with it, including actions taken as a result of the flag/report (see paragraph 4.72). Additionally, we say that it is important that the overall process is sufficiently simple to encourage user engagement (see paragraph 4.74). Ofcom does not believe any amendments to the guidance are necessary for this.

3.135   In relation to views on the reference to 'appropriately timely' within our guidance, it is for VSP providers to consider what an appropriate response time is for their platform. The types of services available are too disparate for Ofcom to suggest or impose a timeframe across all in-scope VSP providers. While this is the case, we have amended the guidance to recommend that VSP providers consider setting internal timeframes for responding to harmful material being reported or flagged (see paragraph 4.75 to 4.76). We also continue to consider that platforms should have the systems to inform users how their report has been dealt with.

3.136   In terms of the comment from the **NCA** around not reporting illegal content to the user due to the possibility of them then destroying evidence, we have strengthened the guidance (see paragraph 4.71) to state that in order not to prejudice any criminal investigation, it may be appropriate for platforms to provide that outcomes for illegal content that it has reported to the police will not be proactively notified to the uploading user.

What respondents said about flags being categorised and recorded

3.137   One VSP provider highlighted that reducing friction in the reporting process increases the number of reports. They said the reporting process needs to strike a balance between having different reporting categories and being clear and simple with only a few steps. They recommended as few reporting categories as possible.

3.138   The **Samaritans** stressed the importance of having self-harm and suicide specific reporting categories.

3.139   **Tech Against Terrorism** recommended a tiered approach to reporting whereby platforms would be able to prioritise reports from 'a trusted flagger'.

3.140   The **NSPCC** noted the barriers in reporting child abuse material. In particular, they said it seems likely that additional measures will be required to ensure VSP providers improve their reporting processes. They suggest Ofcom engages with other regulators on identifying sectoral best practice which could include working with user experience and digital delivery teams to produce replicable design patterns for user reporting mechanisms.

Ofcom's response

3.141   Ofcom acknowledges the different views around reporting categories and that some respondents feel that fewer categories would be better, while others feel specific categories would be important. Currently, Ofcom does not have the relevant research on whether fewer or more precise reporting categories are more effective. As such, VSP providers should decide what they believe will encourage users to report content on the service which they believe may be in breach of the platforms' policies.

3.142   Ofcom will continue to work on our understanding of the barriers to reporting and flagging experienced by users, as part of our research as a regulator. We expect to see an increase in awareness of reporting and flagging mechanisms and we will work with VSP providers, industry and research institutions to promote best practice.

3.143   In relation to **NSPCC**'s views around barriers in reporting child abuse material, we will work with others in the child protection space to ensure that the risk of CSAM being uploaded is reduced. We will also work with platforms to understand, and improve where necessary, the processes they have in place for removing it.

3.144   Additionally, in light of the feedback regarding the use of trusted flaggers to be able to report harmful material, Ofcom believes that trusted flaggers often play an important role in either flagging content themselves or on behalf of users who have approached them. We have therefore added guidance around this that explains that VSP providers may want

to prioritise reports from certain users (e.g. specialist charities) to highlight potentially harmful content faster. To the extent they do so, it would be for VSP providers to decide the purpose of a trusted flagger and who they are (see paragraph 4.62 in the guidance).

Systems for viewers to rate harmful material

3.145   Our draft guidance suggested that VSPs should have systems in place to allow viewers to rate harmful material to assist providers in taking steps to ensure restricted material is appropriately labelled and under-18s are protected from viewing it (4.73-4.86 of the draft guidance)

3.146   We acknowledged the risks of accuracy and gaming involved with user-generated rating systems and caution against the use of 'crowd-sourced' rating in isolation from other protective measures.

3.147   The draft guidance distinguishes between rating systems for users, and other protective measures and outlines how these measures can work together. Providing rating systems for content creators is one way that VSPs can implement their requirement (See 4.17 – 4.23 of the Guidance) for uploaders to notify the service of the presence of restricted material. Ratings systems for viewers are currently not widely used among industry but can be used as a reviewing mechanism of the tags or ratings applied by uploaders. For example, we suggested that if enough viewers believe a rating is incorrectly applied this might be amended without intervention from the platform.

3.148   We also suggested to VSPs that where they use access control measures such as age assurance and parental controls, these can be made more effective by tying them to tagging or rating systems. The guidance states that for the material with the most potential to harm under-18s we would expect a rating system to be linked to access control measures.

3.149   We noted that VSPs can use different types of tagging or ratings systems as appropriate for their service; that they may wish to employ established frameworks such as the BBFC and PEGI ratings systems; and should make tagging and rating systems clear and easy to use, with accessible definitions of what different tags and ratings mean and how they should be applied.

What respondents said

3.150   Several respondents supported our guidance on ratings systems. The **Board of Deputies for British Jews** agreed that it was important for viewers to be able to rate harmful material. The **Samaritans** supported allowing users to rate or label content, as it could lead to more straightforward and intuitive mechanisms for users to add content notes and trigger warnings.

3.151   Other respondents expressed concern about misuse and abuse of ratings systems, with several civil society bodies expressing concern about the deliberate misuse of rating systems.

3.152   A civil society body, warned that rating systems are unlikely to work on fringe social media platforms where users are visiting sites in order to access harmful and/or extremist content, as viewers may want to use ratings to reduce the barriers to viewing and accessing harmful content.

3.153   Several respondents expressed concerns around gaming of the system. **5Rights Foundation** said this would be particularly concerning in cases where ratings could be applied without intervention from the platform, recommending the guidance explicitly stated that 'for services likely to be accessed by under-18s, VSPs should not allow viewers to challenge or change the rating of harmful material before being reviewed and approved by moderators.' Two online service providers said that uploaders might try to game the system to benefit themselves or disadvantage others.

3.154   Some respondents, including **SWGfL**, felt viewers might not have the required expertise to appropriately rate content, while the Samaritans warned that self-harm and suicide content does not necessarily fall easily into 'harmful' or 'helpful' categories and different users may perceive the same content differently. **TikTok** argued that ratings are subjective and even well-intentioned users may have low accuracy when rating content. They also highlighted that inaccuracy in user rating could take substantial resource to correct.

3.155   These concerns led some to agree with Ofcom's suggestion that ratings should form one part of a collection of protective measures. **TikTok** had reservations about the use of user-generated ratings in isolation from other classification approaches. Similarly, **Samaritans** said that ratings should be one part of a robust process for assessing and acting on harmful content, rather than safety of users all resting on crowdsourced ratings. **Tech Against Terrorism** noted that rating systems would need to be complemented by some form of proactive moderation to limit the risks of malevolent actors using rating systems to circumvent content moderation.

3.156   Some respondents highlighted a lack of clarity in how ratings can work alongside other measures. **ISBA** suggested that the draft guidance didn't clearly distinguish between those uploading and viewing content.

3.157   One industry respondent noted ambiguity between 'rating' and 'flagging'; they said they felt viewers should be able to 'flag', while uploaders should be able to 'rate' restricted material as inappropriate for under-18s.

3.158   **AVPA** suggested that there was ambiguity in the language surrounding the kind of content for which ratings would not be sufficient and that access controls should also be used. They suggest that the wording "for material which has the most potential to harm under-18s" used at 4.85 in the draft guidance, could imply that there is some content that would be rated R18 or unsuitable for classification and could still fall short of the bar for being defined as having "the most potential to harm under-18s". They suggest instead that the guidance requires 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".

3.159   **Tech Against Terrorism** felt that there was a contradiction between our guidance on reporting and rating. In their view, the reporting guidance tells VSPs that users should be asked to report content that may be harmful, whereas the rating guidance says that this decision about whether content is harmful can be 'crowd sourced'. They ask for clarity about whether platforms should favour user reporting or rating.

3.160   Several respondents commented on how ratings systems should operate. **SWGfL** and the **Liberal Democrats DCMS Team** supported the use of established ratings systems on VSPs. SWGfL felt that using more 'sophisticated' rating systems (e.g. BBFC or VSC Ratings) was a good way of ensuring transparency.

3.161   **TikTok** acknowledged that there was some value in using existing ratings frameworks but recommended the guidance acknowledge there are a number of ways that content may be rated or classified and that each VSP is best placed to determine what method is likely to be effective on its platform. However, **ISBA** encouraged Ofcom to provide guidance for VSPs on what rating system they should be using, and wherever possible this should be consistent across platforms, not at their discretion.

3.162   Some VSP providers suggested that ratings systems would not be appropriate for their service. One said that as 'restricted material' is clearly prohibited in their Community Guidelines and they have moderation systems in place to delete such content where they find it, rating systems are not required. Another said they didn't think it would be appropriate to implement systems that are open to abuse. They expressed concern about systems altering the commercial premise of the site if users can change ratings of content without intervention from the platform. They were unclear as to whether ratings would be tied to access control measures. **Fanzworld** said that there should be no ratings systems, but a clear definition of harmful material.

Ofcom's response

3.163   In our view, viewer ratings systems are unlikely to offer adequate protection if used on their own, but can be effective when used in conjunction with other protection measures to strengthen protection from age inappropriate content.

3.164   We would like to make clear, in light of Tech Against Terrorism's response (3.149), that Ofcom considers the implementation of systems to report and flag harmful content are central to a service's compliance with the VSP Regime. We do not however, consider systems for viewers to rate harmful material as central to compliance.

3.165   We acknowledge that systems that provide for both uploader-generated and platform-generated ratings may provide additional protection for users and that VSPs may wish to consider implementing such systems. However, the VSP Framework refers only to systems allowing *viewers* to rate harmful material.

3.166   Ofcom recognises that misuse and abuse of ratings is a serious concern, especially where there is the possibility for ratings to be changed without intervention from the platform. We have therefore added to the guidance (4.87) to make clear that where such a

functionality exists the VSP would have be confident that their systems were not vulnerable to misuse and abuse.

3.167   In response to the **AVPA**'s comments that there was ambiguity in the language we used to outline how tagging and rating systems work well with other protection measures, we have updated the guidance (4.101 – 4.103) to add clarity. The reason for highlighting the links between ratings systems, and parental controls is to outline how platforms could use ratings alongside parental controls to ensure that under-18s cannot access material that a parent or caregiver has determined to be age-inappropriate. In linking to age assurance, our intention is to demonstrate how age-based content ratings can be used on sites with effective age assurance to support the VSP in delivering age-appropriate material.

3.168   We acknowledge the support from respondents **Liberal Democrat DCMS team** and **SWGfL** for the use of established classification frameworks. We also accept the view given by **TikTok** that in some cases these classifications might not be suitable for a service. We have therefore suggested in the guidance (4.97) that where a VSP is not implementing their own ratings systems they may wish to incorporate established frameworks through partnerships with ratings bodies, such as the BBFC or VSC Rating Board (PEGI).

3.169   We recognise, however, that for adult services ratings systems are less likely to be a relevant protection. It is for service providers to assess whether such rating systems are appropriate for their platform, having regard to the practicable and proportionate criteria in Section 6 of the Guidance (see paras 6.1 – 6.35).

Age assurance systems

3.170   VSP providers are required to apply the principle that restricted material that has the most potential to harm the physical, mental or moral development of under-18s must be subject to the strictest access control measures.

3.171   Our draft guidance stated that VSP providers which have restricted material that is of a pornographic nature should have a robust access control system that verifies age and prevents under-18s from accessing such material. We said that this applies to VSPs which specialise in pornographic material, as well as services which have a high prevalence of such material. The draft guidance sets out forms of age verification which would not be considered appropriate protection measures for material of a pornographic nature.

3.172   We also emphasised that VSP providers should seek to understand, in a privacy preserving way, which age groups are using the service so they can ensure that material is age-appropriate, taking into account the different developmental needs and interests of under-18s.

3.173   We set out considerations for effective age assurance for VSP providers to consider, including: reliability and accuracy of method in relation to the risk; easy integration into the user experience; ensuring mechanisms are not easily bypassed by children lying about age; how different tools such as reporting, ratings and parental controls interact with age assurance measures; the consideration of third-party providers and technical standards; as

well as consideration of the exclusionary risks to children in different environments of specific age assurance methods.

What respondents said about age verification for adult material

3.174   Most respondents from civil society groups agreed that VSPs containing pornographic material and material unsuitable for classification should have robust age verification in place. The **NSPCC** and **5Rights Foundation** supported the principle that VSPs that carry the greatest risks to children needed to have in place the most robust forms of age verification. **5Rights Foundation** recommended extending the list of approaches which Ofcom would not consider to be appropriate age verification to include cross-platform verification and profiling. It also recommended that we should explicitly link a provider's risk assessment to the VSP providers choice of age assurance approach, having regard to the practicable and proportionate criteria. The **Liberal Democrats DCMS Team** said that age verification should be mandatory and there should be strong sanctions if not implemented. It also suggested that Ofcom should work with the BBFC to implement age verification.

3.175   VSP respondents **TikTok** and **Fanzworld** both agreed with our guidance stating that if a VSP has restricted material on its service of a pornographic nature, providers should have a robust access control system in place that verifies a user's age and prevents under-18s from accessing such material.

3.176   **TikTok** and the **NSPCC** asked for clarity on the threshold for defining VSPs with a high prevalence of pornographic material, with both asking for Ofcom to be clearer on the test and its meaning.

3.177   **UK Babe Channels** disagreed with age verification requirements and stated that viewers and uploaders would simply switch to sites that do not require age verification, including major adult platforms (not in Ofcom's jurisdiction). The VSP provider also said that the impact of age verification would put them out of business. One VSP provider challenged the benefits of third-party solutions, citing that they were in an early stage of development. The **Age Verification Providers Association (AVPA)** noted that under the last age verification proposals there was great concern that it would be unevenly implemented and enforced with disproportionate attention paid to a limited number of high profile services and that this would lead to rapid diversion of traffic to sites escaping the attention of the regulator.

3.178   One VSP provider also told us that in their experience these solutions were not as low in cost as the providers claimed. Another VSP provider also told us that age verification systems could be extremely costly to implement and that it could lead to gathering of personal information from users. Another adult VSP provider also cited the lack of a level playing field with VSP providers who would remain outside of regulatory scope, as well as the costs to smaller services of implementing solutions, as potential barriers for VSP providers.

3.179   One adult VSP provider also said that age verification is a clear example of significant cost to the VSP provider if they host pornography on their platform. It said that there does not

seem to be the same rigour to enforce a level playing field to other VSPs to ensure that children are prevented from accessing their platforms and gaining exposure to inappropriate content and therefore online harm.

3.180   In contrast, **Expert Panel on Age Restrictions**, **AVPA** and **1Account** all said that cost should not be a barrier to platforms adopting solutions in an open and competitive market. AVPA added that an age check cost is in pence not pounds and that some providers publish their tariffs. It also said that the pricing is well below the cost of identity checks for Know Your Customer (KYC) rules in other sectors and that, although more complex or novel solutions may not be viable for services with limited resources, there are widely available off-the-shelf age verification tools that are easily integrated plug-ins to the major platforms that services are built on.

Ofcom's response

3.181   We note the responses of stakeholders who raised concerns over the impact of robust age verification on business, however the VSP Framework is clear in its requirement that providers who have material which has the most potential to harm under-18s need have in place the strictest access control measures. Ofcom has determined pornography to be material that has the most potential to harm under-18s, meaning that sites that host such material do require more robust access controls than those that contain material with less potential to harm under-18s.

3.182   We note that respondents have asked for clarification over what would constitute a high prevalence of pornographic material on a service. We have removed the reference to prevalence in the guidance. Where we say that robust access control systems should be in place for pornographic material, we have said that we consider this a priority for VSP providers specialising in pornographic material, VSP providers with services on which there is a significant risk of under-18s encountering pornographic material, and/or VSP providers that allow pornographic material in their terms of service. It is for VSP providers to consider these factors and decide whether robust access controls need to be applied either to the whole platform or a part of it.

3.183   Should Ofcom be required to make an assessment about whether a platform requires such measures, we have included some of the indicators that we might consider in making this assessment at para 4.112 of the guidance.

3.184   We also note the broad support for our expectation that VSPs which have restricted material on their service of a pornographic nature should have a robust access control system that verifies age and prevents under-18s from accessing such material.

3.185   Taking into account some of the concerns raised from industry respondents, we understand that VSPs which host pornographic material may incur additional costs associated with implementing age verification if they do not already have systems in place. We believe that the age verification sector is mature and competitive enough to offer a range of solutions to adult VSPs. This view is supported by publicly available unit pricing

information from third-party providers[10], DCMS' impact assessment for the Online Safety Bill which cites age verification costs, regular engagement with age verification providers, as well as through their consultation responses. We are satisfied that adequate, easily integrated age verification options are available. However, we will consider the impact on smaller VSP providers who suggest that their business may be significantly impacted as a result of age verification implementation. We will do this by working with smaller providers on the practical timelines for implementation of appropriate measures.

3.186   There are constraints to the jurisdictional scope of VSP regulation and as a result of requiring age verification for adult UK-notified services there are potential competitive impacts to consider. Users of these services may be inadvertently driven to use of non-UK providers, where they may not need to verify their age to access pornographic material.

3.187   Whilst we acknowledge these concerns regarding a level playing field and the limitations to the scale of protection Ofcom's VSP Regime to online pornography, VSPs within UK jurisdiction do nonetheless have an obligation to take measures to protect children from harmful material. There is also a range of legislative steps being taken globally to protect children from the risks posed to them through pornographic sites, in particular through the harmonised framework of the AVMS Directive across Europe.

3.188   To capitalise on this, we are accelerating our coordination with a range of international regulators for greater regulatory alignment in the future to bring more consistency for providers. Our aim is to ensure that services without adequate protections will not be able to operate without any scrutiny across international boundaries. We intend to set up an International working group on Age Verification and Age Assurance with other regulators within the next 12 months, to coordinate implementation of these obligations and share best practice.

3.189   The direction of travel in the UK has for some time been towards stricter rules around access to online pornography, and the forthcoming Online Safety Bill is expected to place new requirements on all services receivable to UK users. VSP providers can exemplify good practice through the proactive implementation of appropriate measures for their services ahead of the broader regime coming into force.

3.190   Some respondents have underlined the importance of standards and certification schemes in supporting good practice when it comes to age assurance solutions. Whilst we are currently not setting up a new technical standard or certification scheme of our own, we agree with respondents on the importance of standards and certifications and we believe that such measures can help provide a degree of certainty for VSP, especially those run by smaller or emerging businesses. We will signpost established and emerging technical standards in our guidance and through our ongoing engagement with VSP providers, and we will continue to monitor the role of standards and certification in relation to VSP regulation, as well as part of broader Online Safety proposals as they develop further.

---

[10] Example of the stated cost of £0.45 per age verification from provider VerifyMyAge. The provider Yoti has also issued a £0.25 per verification cost as part of it broader pricing strategy.

3.191   Following the publication of this Statement and the final guidance, we are committed to working with VSP providers to help them improve protection measures and will take a pragmatic approach when it comes to the implementation of age verification solutions. We expect providers to engage constructively with Ofcom. For more information on our planned approach see Ofcom's Plan and Approach document.

What respondents said about age assurance for services accessed by under-18s

3.192   There was a mix of views on age assurance for services where children were likely to be accessing a broad range of material. **Yoti** believed our consideration for VSP providers on how to achieve effective age assurance was comprehensive, while **TikTok** stated support for Ofcom's risk-based approach to age assurance, as well as our considerations around including neutral age-gates and the importance of inclusive and non-disruptive measures.

3.193   The **NSPCC** told us that VSP providers should introduce age assurance technologies to effectively prevent children and young people from harmful material. It also shared a concern that without clearer guidance from Ofcom, VSP providers may not have regulatory certainty to invest in more substantial age assurance mechanisms. **techUK** regarded age assurance as less a technical challenge and more driven by companies' reluctance to gather more personal data of users and increase user friction. It also stressed the importance of respecting the rights of children to participate online and that any measures had to be proportionate to the risks posed to children.

3.194   **TikTok** also welcomed Ofcom's acknowledgment of the limits to how far VSP providers could prevent age-inappropriate material from appearing on a service, and the difficulties of verifying the age of children on the service. It also acknowledged that there is more work to be done by industry on age assurance and that it is committed to working collaboratively with industry peers, regulators and key stakeholders to find solutions.

3.195   Other industry respondents raised the challenges of age assurance, citing the privacy risks to users submitting ID-based data for age verification and the perceived lack of evidence to date of biometric or behavioural age techniques working accurately at scale.

3.196   The role of standards and certification was also noted by some respondents as essential for age assurance, with **5Rights Foundation** stating that the absence of minimum standards in regulation has hampered widespread adoption. Respondents from the age verification sector, including **Age Check Certification Scheme**, supported the view that Ofcom should signpost specific standards and support third party certification schemes as a means to assist VSP providers in showing earned recognition and demonstrating compliance. The **Age Verification Providers Association** told us that early benchmarking would be important in age verification to prevent a "race to the bottom" between platforms. It suggested that a minimum level of age assurance should be defined following PAS 1296.

Ofcom's response

3.197   We acknowledge the challenges facing VSPs when it comes to estimating the age of under-18s using their services. Respondents have underlined the need for VSP providers to have

greater confidence in the age of children and have also outlined the difficulties in doing so. We recognise issues such as data privacy, user friction and public trust in AI technologies as important areas where Ofcom has a shared responsibility with other regulators and industry stakeholders.

3.198 Our approach is to address some of these questions through increased collaboration with key partners such as the ICO and the Centre for Data Ethics and Innovation, as well as the growing safety tech and age verification sector. We also aim to understand further the complexities around age estimation of children through biometrics or behavioural analytics. We are aware of innovative work being done in this area by leading platforms and safety tech companies and we will collaborate with these stakeholders to share our learnings, where appropriate, and promote best practice for VSPs, as new and emerging solutions develop at pace.

3.199 Our wider goal for age assurance is to also encourage those VSP providers who have considerable resource to invest, innovate and research in emerging safety solutions that include AI-driven age estimation technologies. We believe that advancements in technological solutions adopted by leading VSPs would benefit the industry and lead to better outcomes for user safety overall.

3.200 Raising protections for under-18s is one of Ofcom's priority areas of focus for the first twelve months of the VSP Regime. We will aim to understand the safety measures in place in response to the risks present on VSPs that are popular with under-18s, so that there may be a more age-appropriate experience for children of different age groups.

3.201 International coordination is also a priority for Ofcom in the first twelve months. We will continue discussions with national regulatory authorities across EU member states and plan to both formalize bilateral partnerships as well as establish the aforementioned working group on age assurance.

Parental control systems

3.202 Our draft guidance stated that providers offering services to under-18s should strongly consider having some form of parental control feature to support their overall protection measures for under-18s. This could involve enabling parents to place restrictions on the type of content that children are able to see as well as being able to restrict who can view the child's uploaded content.

3.203 While this regulation focusses on video content, user protection can be enhanced through restrictions on other features such as screen time, direct messaging and privacy. VSPs should not rely on parental controls being applied at the network or device level.

3.204 We noted that VSPs can take a flexible approach to parental control tools but should consider a number of factors (see 4.113 a-g of the draft guidance):

a) Trust based dynamic between caregiver and child

b) Paired accounts and password protected features

      c)   A child's ability to circumvent protective measures

      d)   Children's online autonomy

      e)   Links to age assurance

      f)   Links to rating systems

What respondents said

3.205   There was support for the use of parental controls by several respondents. **SWGfL** supported the draft guidance on parental controls, and said they are an important measure. **Fanzworld** said there should be parental controls, however they stated that these should be enforced by fines/prosecution of parents.

3.206   Two online service providers demonstrated their support for the protection measure by outlining their own parental control measures. This included **TikTok** who said that parental controls are effective and agree with Ofcom that a trusting relationship between parent and child is the key to the success of parental controls. They argued that as this relationship is not something that the platform can have control over, the platform's compliance measures should not be perceived as lacking if there is a low take-up of parental controls.

3.207   There were a number of concerns around parental controls from the age verification sector, including: parental controls not being proven as effective as measures for preventing and protecting under-18s from accessing or being exposed to harmful or unsuitable content; parental controls not being an inclusive measure; parental controls not taking account of socio-economic differences, language barriers, levels of digital literacy amongst parents as well as children in care; and, parental controls are only effective where parents have the knowledge and will to use them and that where they are available parents often don't use them.

3.208   **5Rights Foundation** also expressed concern about how well-placed some parents were to protect their children.

3.209   Several respondents argued that, because of these drawbacks, parental controls should only form an additional layer of protection alongside other measures. **Age Check Certification Scheme**, **Expert Panel on Age Restrictions**, **1Account** and **AVPA** all said that parental controls should form an additional level of protection. Expert Panel on Age Restrictions suggested that parental controls should be supplementary to awareness raising among parents about harms and safety-by-design measures by providers. 1Account and AVPA said that parental controls should not be seen as a substitute for age-verification controls.

3.210   **5Rights Foundation** expressed concern that the guidance 'gives age assurance and parental controls equal weighting'. They suggest this allows VSPs to defer responsibility to parents and carers, instead of making their services safer by design by default.

3.211   **5Rights Foundation** also do not support an approach which requires all VSPs with child users to offer parental controls, as they feel this risks undue interference from adults and

instead recommends that account holder confirmation (paired accounts) and parental controls are included as alternatives to age assurance, only in limited cases where age assurance is not possible or not appropriate.

3.212   **techUK** stated that Community Guidelines and enforcement mechanisms can allow for parents and users to have greater trust in the different platforms and services.

3.213   Two VSP providers felt it would not be appropriate for their platform to offer parental controls, as they use age-gating to ensure users are over a certain age.

3.214   Several respondents emphasised the importance of the digital autonomy of children and giving teenagers a higher level of autonomy online. **5Rights Foundation** highlighted the possibility of parental controls limiting the digital autonomy of some children. In mixed age families, older children can have their digital experiences limited by controls set to protect younger family members. **TikTok** said when designing their Family Pairing feature, they were mindful of the need to take into account the rights of children and encouraged Ofcom to emphasise the rights of children in the guidance on parental controls.

3.215   [✂]

Ofcom's response

3.216   We consider that parental controls can offer an important tool to allow parents and carers to feel confident that their child is using a VSP within safe parameters.

3.217   We understand the point raised by **5Rights Foundation** in relation to parental controls that the involvement of parents may not always work in the best interests of the child. We have made changes to the guidance (4.135- 4.141) to emphasise the importance of affording children autonomy online and ask VSPs to consider the different needs of younger and older children. We also make clear that in principle parental controls should not be a system to monitor and restrict, but to give parents the option to set safer boundaries within which a child can use a VSP.

3.218   Several other respondents raised a similar point about caregivers not always being best placed to protect children online. We ask VSPs to be mindful of the circumstances of all children when designing their safety measures. As such we have updated the guidance (4.135) to ask platforms to consider using media literacy tools to assist caregivers in using parental control technology effectively. We also now acknowledge in the guidance that parental controls should form part of a broader safety net of measures so that for children without caregivers able to use parental controls, there are still adequate protections in place. In addition to this, we ask that platforms are considerate of the kind of information that can be shared with parents, for example, access to helplines for children with abusive parents. We encourage this to be done in the spirit of designing parental control tools that set boundaries rather than creating a system of monitoring and restriction.

Complaints process

3.219   The draft guidance explained that the VSP framework refers to establishing and operating a complaints process relating to: flagging and reporting mechanisms and the explanations associated with them; systems for users to rate harmful material; age assurance systems; and parental control systems.

3.220   We recommended that where a VSP provider adopts a complaints process, they consider whether it should cover all aspects of user safety and should be available to both users and non-users.

3.221   We said that the complaints process must be distinct from the dispute resolution procedure and that the complaints process would typically, although not always, precede a dispute claim. The draft guidance also outlined how complaints processes should be transparent, easy to use and effective.

What respondents said

3.222   Of the notified VSPs that responded, all provided details of their existing complaints frameworks. **TikTok** said it was important that users are able to raise concerns with VSPs but would welcome confirmation from Ofcom that it would not hold VSPs to account beyond the standards required in the legislation. It also said VSPs should have discretion to handle complaints as they see appropriate, for instance in the case of vexatious complaints. Another VSP provider was concerned about encouraging large numbers of complaints that might be vexatious. One VSP provider said that the complaints process recommendations in the draft guidance were sensible.

3.223   **techUK** said it would be helpful to understand whether VSP complaints data would be required on a general basis in relation to Ofcom's monitoring. In its consideration of how a VSP should set out its complaints process, it said it would be useful to understand whether distinctly different measures related to complaints frameworks should be taken for vulnerable users.

3.224   Respondents representing civil society and other organisations felt that a complaints process was necessary. **SWGfL** said that the distinction between complaints and dispute resolution in the guidance was helpful and recommended the use of clear language when describing complaints functions. **IMPRESS** said that Ofcom had not gone far enough in its guidance and VSPs were likely to adopt the minimum standards required to comply.

Ofcom's response

3.225   The guidance makes clear that the legislation states that where VSPs have a complaints process in place, it must relate to the following measures: flagging and reporting mechanisms and the explanations associated with them; systems for users to rate harmful material; age assurance systems; and parental control systems.

3.226   Ofcom's purpose in suggesting that providers consider applying complaints processes more broadly, is not to broaden the scope of this measure in the legislation, but to set out what,

in our view, would be best practice if a VSP chooses to go beyond the legislative requirements.

3.227   VSP providers have flexibility and discretion under the VSP Framework to assess which measures it is appropriate to take and how to implement these effectively. For example, VSPs are able to handle vexatious or repeated complaints as they see fit.

3.228   In relation to **techUK's** question about whether VSP complaints data would be required on a general basis as part of Ofcom's monitoring, we discuss our approach to monitoring in Section 8 of the guidance and below at paragraphs 3.345 – 3.357. We consider data and information relating to complaints to be potentially helpful in assessing the effectiveness of measures.

Dispute resolution process

3.229   The draft guidance outlined that the legislation requires VSPs to have an impartial dispute resolution procedure in place relating to the implementation of any measure set out in Schedule 15A, or a decision to take, or not take, any such measure.

3.230   We said that it was for VSPs to ensure the procedure in place meets the requirements of the regime and that VSPs may take different approaches in doing so depending on the nature of the service and its size (referencing Section 5).

3.231   The draft guidance proposed that VSP providers should be able to demonstrate, at a minimum, procedural separation between their complaints or reporting processes and their dispute resolution procedure. We said that at the very least, this should involve separate individuals dealing with the original complaint and the related dispute. However, in some cases the most effective means of achieving impartiality may be an external, fully independent decision-making body or person. We also said that platforms may employ an appropriate third party for the mediation of disputes with users. We noted the developing nature of this sector and said that we were supportive of innovation in this area.

3.232   We said a VSP provider's dispute resolution procedure should allow users to challenge decisions taken by the provider and to seek redress. We gave examples of potential dispute resolution claims, including: content removal, and account suspension or blocking decisions. We also suggested examples of potential outcomes, including: reinstating or removing content, sanctions against offending users, issuing apologies or corrections, and changes in policy.

3.233   We said careful consideration should be given to disputes about videos containing news content and videos uploaded by broadcasters. We said it may be appropriate for some VSPs to consider an expedited process for disputes from broadcasters and other media outlets.

What respondents said

3.234   Of the notified VSPs that responded, **TikTok** was concerned that the guidance went beyond what is required in the legislation. It said that the legislation does not require the

procedure to apply to individual content decisions taken by a VSP and that it should only be required to settle disputes that relate to whether and how VSPs have implemented the appropriate measures. "Those measures relate to actions taken by VSPs to include certain terms and conditions, to provide functionality and to establish and operate mechanisms, systems and procedures. They are not measures requiring VSPs to take particular decisions about content or to take decisions in a particular way. The Act does not, therefore, require the procedure to be available for resolution of disputes about decisions taken by VSPs in individual cases under the measures they have implemented."

3.235   **techUK** also said that the draft guidance went beyond what was required in the legislation regarding the removal of content being handled by a dispute resolution procedure. It noted the "significant scale" of content removed every day and said that allowing removal of content to be disputed by users could overburden VSPs. It also said that it and its members agreed that impartial dispute resolution procedures can play an important role in some instances.

3.236   **TikTok** felt the draft guidance was disproportionate, in particular given the likely short-lived nature of the VSP Regime. It flagged concern about potential use of a third party for this function in relation to the sharing of user data and GDPR. Other VSPs also raised concern about this requirement being potentially costly, burdensome and in some cases not relevant to VSPs and open to frivolous, repeated or vexatious disputes. TikTok also recommended Ofcom include guidance on procedural requirements of the dispute resolution procedure and highlighted features used for dispute resolution in other sectors. Another respondent said it was concerned the guidance was disproportionate and recommended VSPs be able to stipulate that complaints processes be exhausted prior to making a dispute claim.

3.237   Another VSP provider was concerned that prompting users to raise a dispute when enforcement action is taken would have significant repercussions on staffing and workload for platforms with large user numbers. It also said use of a third party for this function might make platforms less accountable for the decisions taken to keep users safe.

3.238   [✂]

3.239   Civil society respondents said that a dispute resolution procedure separate from the complaints process was necessary. **SWGfL**'s response provided information about its Report Harmful Content service[11], which provides advice to individuals about how to report harmful content online and further actions that can be taken once an individual has already engaged with a provider. It said that in order to ensure an impartial procedure, external separation would be required to demonstrate impartiality and achieve fairness and transparency. SWGfL also signposted the financial sector, in which individuals are made aware of the Financial Ombudsman Service at the conclusions of their complaint and suggested VSPs should be required to signpost users to the dispute resolution procedure at that point.

---

[11] In its response SWGfL referred to its Report Harmful Content 2020 Annual Report

3.240 **IMPRESS** said that Ofcom had not gone far enough in its guidance and said that VSPs are likely to adopt the minimum standards required to comply. It said internal appointments were unlikely to lead to impartial decision-making and that compliance should be administered by a secretariat not employed by the platform. It also said a review measure should be built into Ofcom's oversight role with the option to enforce stricter requirements.

3.241 **5Rights Foundation** suggested that certain types of harmful material, specifically protection of under-18s, should be prioritised and able to be 'fast-tracked'. Others said that while protection of user rights was necessary, the guidance placed a heavy and disproportionate burden on VSPs.

3.242 The **BBC** welcomed Ofcom's suggestion that some platforms should consider having an expedited process for the handling of disputes from broadcasters, but wanted to see Ofcom give a firmer steer on requiring this separate process for PSBs/trusted news providers as default.

3.243 **Tech Against Terrorism** said the guidance was "unrealistic and impractical" and that it would not be reasonable to expect each VSP to implement its own effective dispute resolution procedure that complied with the guidance. It suggested that to see effective and impartial dispute resolution by VSPs, Ofcom should take on the requirement.

Ofcom's response

Requirements of the legislation

3.244 Ofcom notes that some respondents said the dispute resolution procedure should not include individual content removal decisions.

3.245 The legislation sets out that the requirement for an out-of-court procedure relates to the resolution of any dispute between a person using the service and the provider relating to the implementation of a measure or a decision to take, or not to take, a measure. The purpose of the measures in the VSP framework is to protect users from the harms specified in the legislation. The way in which measures are implemented and the measures that a VSP provider decides are appropriate to take, or not to take, are therefore intrinsic to securing user protection.

3.246 Ofcom considers that users are likely to have a particular interest in the way a measure is implemented when this results in a decision being taken by a VSP that impacts them. This may be the case, for example, if a provider's implementation of a measure results in a decision about a user's content that they do not agree with.

3.247 A VSP provider's decision to take or not take a particular measure may also affect users, particularly where a user feels their rights and interests have not been taken into account. We have included more detail in the guidance on what a potential dispute of this nature might involve.

3.248 Additionally, the legislation also requires that the provision of an out-of-court dispute resolution procedure must not affect the ability of a person using the service to bring a

claim in civil proceedings. Ofcom considers that any claim a user is likely to bring in civil proceedings against a VSP would be one that concerns a matter that related directly to them, for example the impact of any action or inaction taken by a VSP. In some instances, this may relate to individual content decisions, for instance a VSP's decision resulting from implementation of its terms and conditions.

3.249   [✂]

3.250   Having taken all responses into account, we have added further detail relating to disputes about a VSP's decision to take or not take a particular measure and what this might involve. We have also provided clarity by amending the examples given in the guidance for potential dispute and potential outcomes of dispute resolution procedures.

Potential burden to businesses

3.251   We also acknowledge that some respondents were concerned about the cost and potential burden this aspect of the regime might place on VSPs. Ofcom is mindful of the potential impact on VSPs of differing sizes and we have carefully considered the requirement imposed by the legislation and how we will secure compliance throughout the drafting of the guidance. While we acknowledge this requirement may pose a challenge for VSPs, nonetheless in passing the AVMS Regulations Government and Parliament have made it a statutory requirement that must be put in place by all VSP providers. We have emphasised this in the guidance.

3.252   Some respondents suggested that in order to mitigate the risk of VSPs being inundated with disputes, users should be required to have exhausted a complaints process prior to engaging with a dispute resolution procedure. Ofcom acknowledges that this may be a practical approach for VSPs to take if they have a comprehensive complaints process in place. However, unlike the requirement to provide for an impartial dispute resolution procedure, complaints procedures are not mandated under the statutory framework. Taking this into account, we have amended the guidance to reflect the fact that it is at the discretion of the VSP provider if they wish to put criteria or stages in place, such as a user needing to have exhausted the complaints process, as part of its dispute resolution procedure. We have also made clear the importance of VSPs having flexibility in how they choose to comply with this requirement.

3.253   In our consideration of responses from VSPs and other industry stakeholders, we have taken into account that some platforms have appeals procedures in place. It is possible that an existing appeals procedure may be an effective method of meeting the dispute resolution requirement, provided it allows for the "resolution of any dispute between a person using the service and the provider relating to the implementation of any measure set out in Schedule 15A, or a decision to take, or not to take, any such measure", is impartial, and does not affect a user's ability to bring a claim in civil proceedings. Having considered this, we have added a reference clarifying that a VSP provider's existing appeals process may be able to be modified to meet the requirement in the guidance.

3.254   Given the concern from some respondents about this aspect of the regime being unduly burdensome, we have amended wording in the draft guidance in which we set out what we considered to be the most effective means of a VSP achieving impartiality. We do not consider there is a single most effective means to ensuring impartial decision making on disputes given the range of services and the lack of existing procedures to draw upon for evidence of effective impartiality in this area. In the guidance, we instead acknowledge that a diversity of approaches may be possible and provide examples of potential approaches that VSPs may wish to take and what things a VSP provider may wish to consider in designing and providing its dispute resolution procedure.

Other areas of consideration

3.255   Ofcom has considered concerns by VSPs operating in the EU that different requirements for dispute resolution procedures might apply in other jurisdictions and that it would be unreasonable to expect VSPs to create different structures for different jurisdictions. The UK legislation derives from the harmonized framework of the AVMS Directive which requires that "Member States shall ensure that out-of-court redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers relating to the application of paragraphs 1 and 3" (Article 28(b)(7)). While different Member States may therefore take different approaches to their own transposition, the underlying requirement for dispute resolution relating to the taking and application of "appropriate" measures remains consistent. Recognising that the UK Government, in its transposition of the Directive, opted to place this requirement on the VSP provider (not the regulator, so Ofcom is unable to perform this function itself), we have sought to provide as much flexibility as possible as to how individual VSPs can achieve this.

3.256   Ofcom notes **TikTok's** concern about potential use of third parties leading to issues in relation to the sharing of user data and GDPR. Ofcom does not consider this prevents the use of a third party given that consent to share data could be sought from users at the time of making a dispute. We also consider that it would be for the VSP to ensure its use of any third party is compliant with other regulation.

3.257   Ofcom has taken into account the views of respondents who said that Ofcom should set more prescriptive guidance with higher standards of compliance and impartiality of the dispute resolution procedure for VSPs. We acknowledge some respondents said impartiality will not be achievable if a dispute resolution procedure is in-house. However, we consider that the guidance explains clearly that VSPs will be required to demonstrate procedural separation between the handling of a complaint and the related dispute. Ofcom considers the positioning in the draft guidance is appropriate given the diversity of services that might fall within scope of the VSP framework and the need for VSP providers to have flexibility and discretion in how they comply with the statutory framework. This flexibility also reflects the legislation which requires that the procedure must be impartial but doesn't stipulate that it must be independent.

3.258   Ofcom has taken into account examples of similar processes from other sectors raised by respondents. These provided helpful procedural examples which we have considered in our inclusion of criteria or stages that VSPs may wish to consider, as discussed above in paragraph 3.252. There may however be a range of ways that VSPs may choose to develop their approach to this requirement that is specific to this industry, which we have made clear in the guidance.

3.259   In its consideration of these points, Ofcom is conscious that the VSP Framework is expected to be superseded by the future Online Safety legislation (see paragraphs 2.23 and 2.24 of the draft guidance) and that the Government has signalled that it does not intend to include an independent resolution mechanism in its proposed legislation. Ofcom is mindful of this and the potential impact of this requirement on VSPs of differing sizes. We have amended the reference in the guidance to future Online Safety legislation to make clear that we will engage with VSP providers to understand and overcome challenges, including practical timelines for implementation.

3.260   In consideration of the responses in the round, we have moved the placement of the dispute resolution procedure to a new section in the guidance to provide clarity that this is a requirement that must be put in place by all VSPs, and not a measure for VSPs to take as appropriate to protect users from harmful material.

Media literacy tools and information

3.261   The draft guidance referenced Ofcom's definition of media literacy and stated that media literacy has the potential to help protect users of VSPs from harmful material by encouraging safe use, critical understanding, and responsible creation.

3.262   The draft guidance then set out three key areas for VSP providers to consider when designing and implementing this protection measure:

   a)   The specific tools and information needed to improve their users' media literacy based on the nature of the service and the types of users on it.

   b)   Raising awareness of media literacy tools and information.

   c)   Understanding the effectiveness of media literacy tools and information.

3.263   The draft guidance set out further considerations for VSP providers designing and implementing this and other protection measures:

   a)   Applying the five overarching principles of "effective, easy to use, fair, transparent, and evolving" as set out in paragraph 4.9 of the draft guidance when designing and implementing media literacy tools and information.

   b)   Taking a holistic approach to media literacy by recognising that it is a relevant consideration when designing and implementing other protection measures.

   c)   Applying a framework like the COM-B model to identify behavioural barriers that might limit the effectiveness of chosen protection measures.

What respondents said

3.264   Some responses to the consultation suggested that we could usefully make additions to this section of the guidance.

3.265   Of the notified VSP providers that responded to our consultation, one VSP provider said that they would welcome the inclusion of the types of content that VSPs would be expected to produce and **TikTok** welcomed our approach to enabling VSP providers to decide what tools and information might be most appropriate for their service.

3.266   Of the non-VSP provider respondents, the **BBC** said there was a need for the source of content to be checkable; **The Samaritans** said that all platforms should host or signpost accessible resources relating to self-harm and suicide content, and that awareness should be raised in the three settings we outlined for raising awareness; **5Rights Foundation** said that we should explicitly refer, when discussing the COM-B model, to the evolving capabilities of children and recognise that they have different developmental needs with media literacy tools and information pitched as appropriate; and **5Rights Foundation** further suggested that we explicitly include persuasive design features as a risk of using VSPs.

3.267   Some responses to the consultation suggested that we could usefully supplement this section of the guidance with additional resources. **techUK** thought that we could make some of the guidance on media literacy available in a consumable and useable format, which would be helpful for smaller VSP providers, **Tech Against Terrorism** said that we could create a microsite containing all the media literacy guidance that we wanted platforms to convey and require VSP providers to link to it because our existing approach could be costly and time consuming for most platforms.

3.268   Some responses to the consultation also asked questions about or made comments related to Ofcom's broader approach to media literacy.

Ofcom's response

3.269   Ofcom considers that each VSP provider is best placed to understand the tools and information they should produce under this measure, including their format and focus, based on the nature of their service (including functionality), the types of users on their service (and their needs), and the types and prevalence of harmful material on their service. The guidance therefore provide VSP providers with a non-exhaustive list of areas that they should consider focusing tools and information on, while enabling each VSP provider to decide on the specifics of what they should provide to improve their users' media literacy.

3.270   We note responses regarding the importance of media literacy in combating specific types of harm. We think that tools and information that improve users' media literacy can help to protect users from a range of different harms, including those identified by the **Samaritans**. As above, we think that each VSP provider is best placed to decide on the specific tools and information that they provide to improve media literacy, including any

harms that those tools and information focus on. We have made a small addition to paragraph 4.161 a) iii) of our guidance to reflect this.

3.271   We considered the **BBC**'s response that there is a need for the source of content to be checkable. We think that identifying the source of content can be a key component of critical understanding and that it can help users in deciding whether they want to view the content or how they should interpret the content. VSP providers should consider tools and information that help users to identify the source of content, where appropriate, and have made an addition to paragraph 4.161 b) ii) of our guidance to reflect this.

3.272   In response to **5Rights Foundation**'s comment on persuasive design features as a risk of using VSPs, we note that paragraph 3.13 of our guidance sets out some potential harms that VSP providers might want to consider when determining which measures might be appropriate to take to protect under-18s from material that might impair their physical, mental or moral development, including persuasive design features such as nudging and targeting leading to a detrimental impact on under-18s. We have amended paragraph 6.161 a) iii) of our guidance to reflect that the possible risks of using VSPs might include encountering the harms set out in Section 3.

3.273   We agree with **5Rights Foundation**'s suggestion that we should explicitly refer to the evolving capabilities of children and their developmental needs when discussing the COM-B model, meaning media literacy information and tools should be pitched at an appropriate level. We have amended paragraph 4.166 of the guidance to reflect this.

3.274   We considered responses from stakeholders that suggested that we could supplement our guidance with additional resources for VSP providers, particularly to help providers of smaller VSPs. We will keep under review the usefulness of this guidance, particularly for smaller providers, and will consider what further information, additional advice or workshops might be useful for VSP providers.

3.275   We have taken into account **TikTok**'s request that we acknowledge the potential legal and privacy restrictions that could restrict VSP providers from collecting or sharing quantitative data on users, tools, and campaigns. We think that it is important that VSPs take steps to ensure they are adequately considering the risks of harmful material on their platform and that where VSP providers adopt the media literacy protection measure, they evaluate how effective the tools and information that they provide are at improving media literacy to satisfy themselves (and us, in supervisory or enforcement discussions) that the implementation of this measure is appropriate and effective.

3.276   We have made an addition to paragraph 7.51 of our guidance to reflect that VSPs should consider measuring the effectiveness of tools and information to improve media literacy, and that feasibility considerations regarding quantitative data also apply in this context. Additionally, paragraphs 6.30 – 6.32 of the guidance asks VSP providers to take into account the rights and legitimate interests of users when taking, implementing or assessing the effectiveness of protection measures to ensure they are proportionate. Some of these rights and legitimate interests may be covered by other regulatory regimes, for example users' rights to privacy and data protection are covered by GDPR.

3.277   We considered **TikTok**'s response highlighting the role that Ofcom can play in relation to facilitating the sharing of best practice and responses from other stakeholders relating to our broader role in media literacy and approach to it.

3.278   Ofcom has a statutory duty to promote media literacy and to conduct research in relation to media literacy. In July 2019 we established our Making Sense of Media programme to help improve online media literacy by further developing our extensive research programme and by encouraging collaboration and coordination between relevant stakeholders and their activities. As part of this programme we created the Making Sense of Media Panel, made up of media literacy experts, to help inform the development of our media literacy research and policy, and the Making Sense of Media Network to facilitate information and knowledge sharing across relevant stakeholders. Members of this Network share information, including new resources and research, with each other through our regular Making Sense of Media bulletin.[12]

3.279   We encourage VSP providers to join media literacy networks and, where feasible, to share the results of their evaluation of media literacy tools and information with others. This would enable generation of a collective body of evidence that can inform best practice to improve media literacy and would help to facilitate a coordinated, multi-stakeholder approach to improving media literacy.

Determine which measures are appropriate (the practicable and proportionate criteria)

3.280   Under the VSP Framework, VSP providers are required to determine whether it is appropriate to take a particular measure to protect users from harmful material taking into account the factors set out in the Act.

3.281   In addition, when determining whether a measure is appropriate, VSP providers must apply the principle that restricted material that has the most potential to harm the physical, mental or moral development of under-18s must be subject to the strictest access control measures.

3.282   What is practicable and proportionate must be considered in the round and weighed against the risk of harm to users on a platform.

What respondents said

3.283   In general, respondents were supportive of the proposed guidance on the criteria set out. Several emphasised the importance of all criteria being considered in the round, and that "any other measures" taken are to be included in the VSP's assessment.

3.284   There were concerns about how a VSP's size is considered in the assessment. A VSP provider highlighted size as a central factor in assessing what will be practicable and proportionate, while **Tech Against Terrorism**, **SWGfL** and **5Rights Foundation** stated that

---

[12] Making Sense of Media bulletins - Ofcom

smaller and less-resourced services may be targeted as hosts for harmful content, or have users driven to them by stricter age-verification enforcement on larger services. For example, **5Rights Foundation** has recommended removing "size" from 5.1, as a smaller service is not necessarily a safer service. **TikTok** and **Fanzworld** stated that measures should be implemented in proportion to the size and nature of the provider.

3.285   There were some calls for more support for services. **Tech Against Terrorism** argued that service providers are poorly equipped to understand and assess the risk of content, especially terrorist content. They suggest Ofcom provide cross-sector support, and that its current training materials could be adapted to support smaller platforms. **techUK** suggested we could follow the ICO in providing illustrative examples.

3.286   Two providers, **TikTok** and one other VSP provider said that "other measures" taken should be considered in the assessment of what is practicable and proportionate.

3.287   **TikTok** contested paragraph 5.1 of the draft guidance, arguing that services do not have control over the dissemination of content outside their platform, and therefore should not be required to consider it in any assessment or appropriate protection measures.

3.288   The **BBC** proposed that VSPs give special consideration to PSB content when applying protection measures and said it would welcome improved tools for monitoring and moderating user comments on their own channels on social media platforms.

3.289   The **5Rights Foundation** proposed we add a clause on the UN Convention on the Rights of the Child to the section on the interests of the users after paragraph 5.32 in the draft guidance.

3.290   The **National Secular Society** called for more explicit protection for material that is in the public interest, as covered in paragraph 5.35 of the draft guidance.

Ofcom's response

3.291   As a result of the differing responses on the size of platforms we made some minor revisions to the guidance to further emphasise that VSPs must assess how to implement measures in a way that protects their users and is practicable and proportionate to the risk to users. Size is one of many criteria listed in the Act, and so will need to be considered by VSP providers. Size can be determined through a range of metrics, including reach of the platform and volume of content. Resources may also be an important consideration.

3.292   In response to requests for more support for services, we first direct providers to Section 7 of the guidance "Additional steps to protect users". The suggestions on external engagement and especially implementing a risk management process will assist services in meeting their obligations to protect users. We have increased references to this in the guidance. Ofcom will continue to work with providers and stakeholders to ensure the objectives of the VSP Framework are met. We are considering what further support VSP providers may find useful following the publication of the guidance.

3.293   In response to **TikTok's** point, Ofcom confirms that the factors services are required to consider when assessing what measures to take are set out in the Act and include "any

other measures which have been taken or are to be taken".[13] Ofcom will therefore also take this into consideration.

3.294   We have considered **TikTok**'s request to remove the consideration of the reach of content. Once content has left the control of the platform its reach still contributes to the total harm it can cause. Therefore, this risk of harm should be considered in providers' decisions about how to implement protection measures.

3.295   We acknowledge the **BBC**'s concern for their duty of care to users of its social media channels. The BBC's suggestion for improved tools for moderating user comments is beyond the parameters of the regime, which is focused on measures to protect users from audio-visual content. Ofcom recognises the importance of digital services for Public Service Media and would welcome services working together with the BBC and other PSM providers. Our recommendations to support PSM in the digital age are set out in our recent report.[14]

3.296   **5Rights Foundation**'s suggestion draws attention to the importance of the best interests of the child in decisions taken to protect them. We recognise the importance and benefits of online experiences for children, and that these must be considered when taking protection measures. However, we have not considered it necessary to add an explicit reference to the UN Convention on the Rights of the Child to the guidance. As the UK is a signatory, both the VSP Framework and other regulatory regimes such as the ICO's Age Appropriate Design Code are consistent with the principles.

3.297   In response to the **National Secular Society**'s concern about material in the public interest being removed, providers have a duty to protect users from restricted material and relevant harmful material as defined in the Act. Providers should consider how implementing any measure will affect the public interest, among other interests. Ofcom cannot give legal advice, but Section 5 and paragraphs 6.30 to 6.35 of the guidance may assist providers in writing and implementing their terms and conditions.

Additional steps to protect users

3.298   Section 7 of the guidance covers additional steps that Ofcom encourages platforms to consider taking, to strengthen protection for users. Although these are not required under the VSP Framework, we consider that platforms taking these steps are more likely to be in a position to secure appropriate protections for users from harmful material. These are:

   a) **Embedding a culture of user safety**, including the governance and structure of an organisation and the promotion of user safety responsibilities.

   b) **External engagement**, including third party content moderation and relationships with charities, NGOs and harms experts.

---

[13] Section 368Z1 (4) of the Act.
[14] Small Screen: Big Debate Statement Recommendations to Government on the future of Public Service Media, 15 July 2021, https://www.smallscreenbigdebate.co.uk/statement

c) **Risk management processes**, which we encourage all providers to conduct in order to determine which measures (and additional steps) are appropriate to protect their users from harm.

d) **Assessing effectiveness of protection measures**, which we encourage all providers to become proficient at. We consider this vital for VSP providers to understand how well they are working to protect users from harmful content. The collection of data and information is an important aspect of this. Such information may be helpful to Ofcom in assessing compliance.

What respondents said

3.299   **TikTok** requested confirmation that VSPs do not have to implement "additional steps to protect users" listed in the draft guidance to comply with the Act.

Ofcom's response

3.300   The "additional steps to protect users" set out in the guidance are not required in order for services to comply with the VSP Framework, but taking them may assist services in securing protections for users. The Act requires VSP services to protect their users from harms that may result from viewing specific categories of material, and affords VSP providers flexibility in how they protect users. Ofcom will take a holistic view of assessing compliance, seeking to understand the totality of platforms' efforts to protect their users.

Risk management

3.301   The VSP Framework does not tell VSP providers which measures to choose beyond saying that they must take such of the measures as are 'appropriate' for the purposes of protecting users from the specified harms and that this must be determined by whether it is practicable and proportionate for the measure to be taken, taking into account the criteria we discussed in Section 5 of the draft VSP guidance. Measures must be implemented in such a way as to carry out the purpose or purposes for which the measure is 'appropriate'. In other words, the measures must also be effective.

3.302   The VSP Framework does not say anything about what activities, processes, institutional arrangements/governance may be helpful to identify and implement measures that are effective, practicable and proportionate. To help VSP providers in this regard, Section 6 of the draft guidance suggested additional steps which we consider platforms could take to strengthen the protection for users and a risk management framework which embeds a safety-first approach.

3.303   We emphasised that risk management is a dynamic process and that risks should be reviewed regularly, with providers habitually considering whether the risks have been appropriately identified and mitigated. We also suggested that it is best practice to record this process.

3.304   We recognised in the draft guidance that risk management is not a requirement under the VSP Framework but noted that the assessment and management of risk will likely form

part of the future online safety regime and is also part of the European Commission's Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act).

The risk management guidance should be a specific requirement rather than just strongly encouraged and should clearly highlight the importance of accountability at senior levels

3.305   Several respondents **5Rights Foundation, Liberal Democrat DCMS Team** suggested that the risk management guidance should be a requirement. **5Rights Foundation** recommended in particular that VSPs likely to be accessed by children should conduct child risk assessments given that this is in the Online Safety Bill. It additionally recommended that the guidance should state that VSP providers are required to: anticipate the risks posed by the design of their service and that the process should involve identifying potential harms on a platform; document decisions about the measures in place to mitigate those potential harms; and measure the effectiveness of those measures. The **Liberal Democrats DCMS Team** said that even if it is not a requirement, it should be strongly encouraged and so wanted paragraph 5.5 of the draft VSP guidance to be strengthened

3.306   The **NSPCC** supported VSP providers adopting a clearly defined risk management process. It noted that while this is not a requirement under the VSP Regime, it is difficult to see how VSP providers could otherwise ensure they have a sufficiently dynamic, targeted risk mitigation regime in place. It recommended that user safety must be hardwired into VSP decision-making, but noted that in its experience, user safety is often siloed within Trust and Safety teams. To incentivise a cultural shift in how platforms understand and respond to risks, it suggested that the guidance explicitly highlight that having clear accountability for user safety at senior levels is an important enabler for VSP compliance.

Ofcom's response

3.307   We note respondents' comments that the risk management guidance should be a specific requirement rather than just strongly encouraged. However, implementing a risk management process is not a requirement under the VSP Framework. We cannot therefore require it as part of the guidance. However, we note the Liberal Democrat DCMS team's comment about strengthening the guidance in this area, so have updated the guidance to make clear we strongly encourage VSP providers to conduct risk management processes.

3.308   While we cannot require VSP providers to implement a risk management process, we do believe that the risk management framework is helpful for how providers can identify and implement measures that are practicable and proportionate and protect users from risk of harm on their platforms. In particular, we see the adoption of a risk management framework and the documentation of it as a useful approach for providers to demonstrably satisfy themselves (and us, in supervisory or enforcement discussions) that they have anticipated risks, identified both current and emergent harms, and considered the effectiveness of those measures.

3.309   Our strong recommendation for VSP providers to implement a risk management framework also reflects our view that the VSP Regime is an important precursor for Ofcom and industry to online regulation.

3.310   We note the **NSPCC**'s comment that in its experience user safety is often siloed within Trust and Safety teams. We also note its recommendation to incentivise a cultural shift in how platforms understand and respond to risks by way of clear accountability for user safety at senior levels. We agree and implicitly encouraged this in our draft VSP guidance. Paragraph 7.6 recognises that clear accountability for safety at senior levels can promote greater consideration of user safety across an organisation.

3.311   In reviewing our draft guidance, we considered that it is important to make this clearer in our step-by-step guide for risk management. Therefore, we have added a fifth step to the suggested risk management framework in the final guidance of 'risk reporting'. Under this step, we encourage VSP providers to communicate risk management activities to senior decision-makers in their organisations. By adding this extra step, we encourage VSP providers to have strong governance and oversight at a senior leadership level of their VSP obligations. This may therefore help to foster proactive risk management that drives a culture of safety. This additional step is set out in paragraph 7.48 to 7.49 of the VSP guidance.

Transparency of the risk management process is important both internally and externally of the VSP and the guidance should provide expectations around engagement with third parties

3.312   The **National Crime Agency (NCA), NSPCC** and **Samaritans** highlighted the importance of platforms being transparent about the way they assess and manage risk and emphasised that platforms should continually evaluate processes internally. They outlined the importance of platforms being informed by third party subject matter experts, with the NSPCC suggesting that platforms should be encouraged to share their risk assessment with the regulator and relevant expert bodies.

3.313   **Tech Against Terrorism** supported the regular review of measures but had concerns about the practicality of smaller platforms conducting meaningful risk assessments given they have limited resources. It recommended therefore that Ofcom should support knowledge-sharing for smaller platforms e.g. by supporting the Tech Against Terrorism Open Source intelligence report monitoring capacity and Knowledge Sharing Platform. **SWGfL** also recommended that VSPs should increase engagement with external NGOs such as SWGfL to develop and implement policies and procedures to protect users.

Ofcom's response

3.314   We welcome the **NCA**'s, **NSPCC**'s and **Samaritans**' comments about the importance of transparency of the risk management process both internally and externally of the VSP. As outlined above, we have added a fifth step to our risk management framework of 'risk reporting'- this explicitly introduces additional internal transparency of the risk management process.

3.315   We note the comments from respondents that VSP providers should increase engagement with external NGOs and the outcomes of the risk management process should also be made transparent externally to relevant expert bodies. We cannot require this under the VSP Framework but in Section 6 of our VSP guidance, we do encourage providers to work with charities, NGOs and harms experts. We hope that in identifying, assessing, planning for and mitigating any risks, VSP providers would draw from relevant expert bodies, thus ensuring that their risk management processes take into account changing societal attitudes. To make this clearer in the step-by-step guide on risk management, we have added a cross-reference to this section in our framework – see paragraph 7.36. We have also noted in our guidance (see paragraph 7.48) that in some industries, risk reporting is made public to engender confidence in the organisation.

3.316   We note **Tech against Terrorism**'s comment about the practicality of smaller platforms conducting meaningful risk assessments. Following the publication of this Statement and the final guidance, we are committed to working with VSP providers to help guide providers in deciding how best to comply with the statutory requirements.

The guidance should emphasise flexibility in meeting risk management expectations

3.317   One VSP provider said that it agreed that assessing the risks to users and developing plans to mitigate and respond to these is critical for keeping users safe. It said that articulating and addressing risks is embedded in their working practices, however its processes may not mirror the exact risk assessment approach in Ofcom's guidance but does achieve the objectives of articulating risks and developing products, features and policies that mitigate these. Given this, it recommended that Ofcom should focus on the overall objective behind the guidance and allow platforms to develop risk management systems and approaches that are most relevant to their services.

3.318   Similarly, **TikTok** responded that assessing and managing risk is core to the approach taken by their Trust and Safety team. It recommended though that due to the unique nature of each platform and the risks that may arise it will be most effective for VSP providers to determine the best method of assessing and managing these areas, in discussion with the regulator.

Ofcom's response

3.319   We note the comments from a few VSP respondents who emphasised the need for flexibility in meeting risk management expectations and focusing on the objectives behind the guidance.

3.320   We agree with this sentiment and have reflected this in paragraph 7.27. In particular, we have emphasised that the step-by-step guide is to support providers but we recognise that individual platforms might approach how they manage risk in different ways, dependent on their own particular circumstances. The key objective of the VSP regulations is ensuring that users are and continue to be protected from harmful material. The VSP Regime affords flexibility for providers in how they choose to achieve this, though we would recommend documenting and reporting this to senior decision-makers in the organisation.

The purpose of this, being so that VSP providers can demonstrably satisfy themselves (and us, in supervisory or enforcement discussions) that they have adequately considered the risks of harmful material on their platform in determining whether the measures they take or have taken are appropriate, taking into account the practicable and proportionate criteria.

Ofcom should consider the alignment of this risk management framework with other risk-based regimes

3.321   **techUK** highlighted that there are multiple forms of international and domestic regulations that have, or are proposed to have, similar risk provisions, such as the Age-Appropriate Design Code, the draft Online Safety Bill and Digital Services Act. It suggested that it would be useful for Ofcom to provide further clarity on how the proposed VSP risk management process might align with these other regulations. In particular, it urged that regulators avoid unnecessary duplication when collecting the same information as this has the potential to overburden smaller companies.

3.322   **Yoti** stated that one of the risks that Ofcom drew out in the guidance is the risk of an individual's privacy being breached. It added however, that this risk does not appear to form a substantive part of the draft guidance around assessing and managing risk. Yoti encouraged Ofcom to add some discussion of adopting age assurance methods which are privacy by design and default to the section.

Ofcom's response

3.323   We are alive to ensuring the alignment of this risk management framework with other risk-based regimes. Through the Digital Regulatory Cooperation Forum, we are working closely with the ICO to ensure that our respective regulatory regimes are implemented coherently and clearly for industry to be able to understand and apply. As a recent example of this, Ofcom and the ICO participated in an industry workshop to discuss risk assessment and management approaches given the close links between our respective regimes.

3.324   With regard to the linkages with the draft Online Safety Bill and the proposed Digital Services Act, these are still at pre-legislative stages but based on what has been published, the assessment and management of risk will likely form part of these regimes. The VSP Regime is an important first step for Ofcom and industry in online regulation and provides an opportunity to build expertise, test and iterate to meet good outcomes for users. We have made an addition to paragraph 7.26 to make this clearer for industry.

3.325   Additionally, the flexibility afforded to VSP providers in how they meet risk management expectations should help providers to find an approach that best suits their own particular circumstances. Our intention in our engagement with VSP providers is to understand their overall approach to risk and safety management. This includes understanding any risk processes companies already have in place, including to meet other regulatory requirements. We then intend to discuss with providers, where necessary, opportunities to build on those processes to achieve good outcomes for users. We consider this approach

should provide assurance to companies working with multiple regulations and we have further clarified this by making an addition to paragraph 7.31 of the guidance.

3.326   We note **Yoti**'s comment that we should draw out in the step-by-step risk management framework the risk of an individual's privacy being breached and encourage the adoption of age assurance methods which are privacy by design and default. As we set out in Section 6 of the guidance, in determining whether a measure is appropriate VSP providers must take into account the practicable and proportionate criteria under the VSP Framework, which includes taking into account the rights and legitimate interests of users. Where legitimate interests may be impacted, protection measures and their implementation need to be proportionate to the harm the provider is seeking to address. To make this clearer, we have added a cross-reference to these paragraphs in the step-by-step guide on risk management – see paragraph 7.44.

The guidance does not sufficiently focus on emergent risks and should do so

3.327   **techUK** recommended that more guidance and explanation should be given to help VSPs respond to new emerging and fast spreading risks. As an example, it mentioned, a piece of emergent content that is constructed in such a way or linked to additional or third-party content that allows it to slip past common safeguarding mechanisms. It argued that in this case the focus is not on preparation but reaction to emergent risks that could not be foreseen. It argued that this is currently not well covered in the guidance.

Ofcom's response

3.328   We welcome **techUK**'s recommendation that more should be included in the step-by-step guide on risk management to cover emergent risks. We agree that this is an area that we hope VSP providers consider in identifying, assessing, and managing risks adequately. We have slightly amended the step-by-step guide to make it clear that we encourage VSP providers to also make efforts to identify, assess and plan for mitigating emergent risks. This can be found at paragraphs 7.35 to 7.37, 7.39, 7.42 and 7.48 to 7.49.

3.329   In our view, emerging risks are a new or unforeseen risk that has not yet been fully understood. We would not expect platforms to have perfect foresight or to be able to anticipate and mitigate all risks that arise. We consider though that it is reasonable for platforms to be alert to the possibility of emergent risks (including for example looking at the risks that have arisen on similar services and/or that might arise according to expert bodies); and to be able to react quickly to these.

Other comments on the risk management guidance

3.330   One VSP provider said it found the guidance on risk assessment particularly helpful. **Fanzworld** set out the measures it has and commented that other VSP providers may find them useful. The **Board of Deputies of British Jews** recommended there be a system in place so that if a user is banned from one platform for egregious behaviour, other platforms are able to pre-emptively ban that user also.

Ofcom's response

3.331   We note respondents' other comments on the step-by-step guide on risk management and their suggestions/recommendations for VSP providers to adopt particular approaches to manage risk. It is important to note that our guidance document should not be seen as a set of compulsory steps but is intended to help guide providers in deciding how best to comply with the statutory requirements. Which measures are chosen and how they need to be implemented will be dependent on the characteristics of individual services. For this reason, we cannot mandate these suggestions/recommendations, but we acknowledge that they could play a part for some firms to manage the risk of harm on their platform.

Measuring effectiveness

3.332   We said that measuring the effectiveness of protection measures is vital for platforms to understand how well they are working to protect users from harmful content. The collection of data and information is an important aspect of this.

3.333   We strongly encouraged providers to collect information about the measures which have been taken and implemented on their platforms and how effective these measures are at protecting users from harmful material.

3.334   We suggested some examples, including quantitative metrics such as volume of reported harmful material, the number of violations of terms and conditions and the number of appeals. We also suggested the number of views on reported material could be important in assessing prevalence of harm.

3.335   We noted that relevant context must be considered with these indicators and suggested qualitative metrics should also be considered.

What respondents said

3.336   Respondents generally agreed that measuring effectiveness was important to protecting users. **5Rights Foundation** stated that the risk management process should involve identifying harms; documenting decisions about the measures in place to mitigate those potential harms; and measuring effectiveness of those measures. **ISBA** suggested that bigger platforms should make a bigger effort to prevent, identify, and mitigate harm and that bigger platforms also have a responsibility to monitor the effectiveness of their efforts, to report on them, and to evaluate and improve.

3.337   **ISBA** also noted that up until recently, the regulatory environment covering online content has lacked robust data and that they fully supported progress toward new regulation enforced by Ofcom.

3.338   One respondent queried Ofcom's approach to measuring the effectiveness of age assurance. The **Expert Panel on Age Restrictions** asked for more clarity on how Ofcom intends to measure effectiveness of age assurance by providers, as the providers themselves will determine what is appropriate, based on risk assessments.

3.339   Some respondents commented on the specifics of measuring effectiveness. The **NCA** said they would like to see transparency reporting to a prescribed timescale, with a summary included in the annual reports and accounts of VSPs and subject to independent verification.

3.340   The **NSPCC** welcomed Ofcom's guidance that VSPs should develop a series of metrics to enable them to measure the effectiveness of their regulatory response. Although the NSPCC said the proposed list is generally sound, they suggested that VSPs should be encouraged to place greater emphasis on the prevalence of harmful material.

3.341   The **NSPCC** went on to suggest that metrics should provide an assessment of: how many users see relevant harmful content before it is actioned; the interplay between exposure to harmful content and content recommendation systems; and the differential exposure to relevant harmful and restricted content, including among children and young people.

Ofcom's response

3.342   In terms of measuring the effectiveness of age assurance, Ofcom may ask to see the decision-making process for platforms who have employed this measure. We encourage this to be included as part of a risk management process as set out in Section 7. Ofcom may use other sources of information, from the provider or elsewhere, should we need to make a determination about the appropriateness and effectiveness of an age assurance measure.

3.343   We also note that many VSPs already produce transparency reports, often in a regular cycle. We have included some examples of the metrics published in these transparency reports in Section 7 of our guidance. We note some of these align with the metrics suggested by the **NSPCC**. Ofcom intends to work with platforms to understand more about how they assess the effectiveness of their measures, including any metrics they collect.

3.344   Ofcom also intends to publish its own Annual VSP Report regarding the measures taken by platforms and how they are implemented. This will use a number of sources of information to provide users with transparency about safety measures on platforms in scope. Ofcom's VSP report is likely to be the first of its kind that will bring transparency across the sector to shine a light on good practice and enable users to compare different VSPs. More information on this can be found in our VSP Plan and Approach document.

Monitoring and enforcement

3.345   Our draft guidance said that one of the ways we will ensure that VSP providers comply with their requirements under the VSP framework is through monitoring and enforcement of the VSP Regime. We set out some of the ways we expect to monitor compliance, using tools, such as: informal engagement including supervision; information gathering; accessing VSPs; and complaints.

3.346   We also said that where we identify concerns, we will consider whether it is appropriate and proportionate to take enforcement or other action, to help protect users from harm.

We set out the situations in which Ofcom could take action and gave examples of the types of indicators we would take into account in considering such action.

3.347 We said that we would usually attempt to work with providers informally to try to resolve compliance concerns before using formal powers. However, we recognised that there may be circumstances where we would consider taking immediate formal enforcement action in the event of a suspected breach and we set out some examples of the types of indicators that may lead to us opening a formal investigation.

3.348 We provided a brief summary of the key stages of a formal investigation and gave examples of some of the sanctions we could impose in the event we considered a VSP was in breach of their requirements.

What respondents said

3.349 We received a number of comments relevant to this section of the draft guidance, some of which have already been addressed in relevant sections above.

3.350 **TikTok** welcomed our encouragement for users to first raise their complaints with VSPs before complaining to Ofcom and would encourage steps in the process to incentivise this. TikTok also requested that Ofcom share emerging trends from direct complaints.

3.351 **TikTok** also requested Ofcom allow time for VSPs to address any compliance concerns Ofcom is alerted to that have not been raised with the platform.

3.352 The **Liberal Democrats DCMS Team** queried whether Ofcom's enforcement guidelines are fit for purposes in regulating VSPs, welcoming the proposal in the Workplan for the DCRF for a centre of excellence to support work in digital markets and encouraging a wider set of digital skills to be built across regulators involved.

3.353 **5Rights Foundation** recommended strengthening language in relation to additional steps for effectively protecting under-18s, by suggesting Ofcom would use the information to support its compliance monitoring.

Ofcom's response

3.354 We note and welcome **TikTok**'s comments and are considering how we could share high level complaint trend information, where it is available. We will be developing our approach to recording and categorising the complaints Ofcom's receives through its complaints hub over the coming months.

3.355 In response to **TikTok**'s ask and as indicated in 8.28 of the guidance, our general approach would be to consider whether it is appropriate to engage with a VSP to support compliance before considering any formal enforcement activity. That said, in view of TikTok's comments we have amended the guidance to note that we would allow a reasonable timeframe for this. However, as we indicate in the guidance, where our concerns are serious, we may move straight to opening a formal investigation. In which case, as also indicated in the guidance, we would follow our enforcement guidelines which set out

Ofcom's process for investigating a suspected breach, including the opportunity for the provider to make representations about the matters under consideration.

3.356 To the points raised by the **Liberal Democrats DCMS Team**; we are working closely with the DCRF and continue to build on our existing and developing internal digital knowledge and expertise.

3.357 We do not consider it appropriate to amend the wording of the guidance in the way that **5Rights Foundation** suggest. The guidance already sets out the types of factors we may consider and, depending on the circumstances of the issue we are looking at, this could include the taking of additional steps.

4. Responses to the impact assessment

4.1   The Impact Assessment (IA) in the consultation focused on the impact on platforms, users and other stakeholders of specific expectations or recommendations on VSP providers as outlined in the guidance. Specifically, we focused on areas where the guidance is more detailed than the underlying legislation.

4.2   Expectations for which we assessed potential costs and benefits included: measures which we consider are central to protect users, and measures which we strongly encourage to support compliance. These are outlined below:

- Measures which we consider are central to protect users

    – Implementing and enforcing T&Cs related to relevant harmful material
    – Uploader notifications of restricted material being actioned by the provider to protect under-18s
    – Effectively implementing a flagging and reporting mechanism
    – Age verification systems for VSP providers that have restricted material of a pornographic nature and/or unsuitable for a classification certificate

- Measures strongly encouraged to support compliance

    – Risk management process
    – Information collection and measuring effectiveness

4.3   Our overall conclusion was that the expectations on VSP providers from our guidance was unlikely to result in material additional regulatory costs for platforms that exceed those previously estimated from the statutory requirements on VSP providers to comply with Part 4B of the Act, and which have already been considered in previous impact assessments.[15]

4.4   Despite this, we did recognise that there may be some differences in the costs for individual VSP providers and in particular that there are likely to be some negative impacts (including costs) on particular platforms to meet the expectations within the guidance.

4.5   We also considered the various impacts (positive and negative) on users, creators, and advertisers and how these expectations may affect the competitive position of VSP providers, including against out of jurisdiction competitors. After consideration of the impact of our guidance, we concluded that the identified costs that may arise from our specific expectations in the draft guidance, do not materially impact stakeholders in a way that is disproportionate to the benefits that are likely to be secured from them.

What respondents said

4.6   We received a range of responses which considered the impact of introducing measures or our impact assessment itself.

---

[15] DCMS impact assessment for The Audiovisual Media Services Regulation 2020 -

Inclusion of the impact of dispute resolution in the impact assessment

4.7   **TikTok** suggested that the impact assessment did not include the impact of an impartial dispute resolution procedure in two ways. In particular, it suggested that we have not taken into account:

- the costs of introducing such a procedure
- the fact that a procedure that lacks clarity could be overwhelmed and have a negative impact on legitimate complaints.

4.8   **SWGfL** also suggested that impartial dispute resolution will be part of an effective flagging and reporting mechanism so should be mentioned in Table 1 of the Impact Assessment. It also suggested that media literacy measures should be included in the impact assessment.

Impact of age verification on smaller VSP providers

4.9   **UK Babe Channels** said that it would be "surprised if there was any available solution which would be an affordable cost for us" as a smaller VSP. It considered that privacy concerns from their users would mean they would visit alternative sites which do not have the same requirements. UK Babe Channels also suggested the age verification expectations will be a "great advantage to the bigger sites because it means that nobody can compete with them". UK Babe Channels also suggested that it has content which is tame by internet standards and more graphic content can be found on alternative sites, which may not be specific adult sites.

Specific impact on VSP providers that host pornographic content

4.10   A VSP provider noted that age verification is a significant cost to VSP providers which host pornographic content. It asked why VSP providers that host pornographic content had been specifically targeted and queried why there was not the same approach to restrict children's access to other VSP providers hosting inappropriate content.

Inclusion of freedom of expression in the impact assessment

4.11   **National Secular Society** thought the risks to freedom of expression should have been explicitly acknowledged in the impact assessment and identified as a key issue.

Other general discussion about proportionality

4.12   The **Liberal Democrats DCMS Team** and **5Rights Foundation** submitted that any costs that come from meeting our expectations in the guidance will be proportionate to the benefits.

4.13   The **Board of Deputies of British Jews** suggested that while there are valid concerns that the potential costs to providers will naturally favour larger platforms (i.e. smaller platforms will have fewer resources to spend on such regulatory requirements), it did not think that this, in and of itself, is enough of an excuse to void such requirements.

4.14   **AVPA** thought that economy of scale will emerge through the cumulative impact of legislation - AVMSD, GDPR, Age Appropriate Design Code and the Online Safety Bill which

all have requirements around age assurance. It also suggested that international interoperability being developed for both age verification and parental consent means that the cost burden of compliance with age-related regulations will fall rapidly.

4.15   A notified VSP provider mentioned that Tables 1 and 2 were helpful overall summaries of measures detailed in the draft guidance.

Ofcom's response

Including reference to dispute resolution in the impact assessment

4.16   We did not previously include a reference to the dispute resolution procedure in the impact assessment. Unlike the list of measures in Schedule 15A, a dispute resolution is a legal requirement under the VSP Framework. Therefore, we considered there was likely to be limited additional impact from expectations outlined in the guidance.

4.17   Following responses to the draft VSP guidance, we have now considered more explicitly the costs and benefits that could result from our guidance on the dispute resolution procedure. This is set out in Table 2 of the Impact Assessment. In particular, we have revised the guidance to make clear that VSP providers may consider different approaches to meeting the legal requirement, depending on their own particular circumstances – see Section 5 of the VSP guidance. In setting out our approach to dispute resolution in the VSP guidance we are mindful of the potential impact on VSP providers of differing sizes and that the VSP Framework is due to be superseded by the future Online Safety legislation. Therefore, we consider that by recognising a range of potential approaches a VSP provider may take, providers have flexibility to develop an approach to dispute resolution that is effective and appropriate for their service.

Impact of age verification on smaller VSP providers

4.18   We note the concerns from the **UK Babe Channels** over the impact of robust age verification on small businesses. However, the VSP Framework is clear in its requirement that restricted material that has the most potential to harm the physical, mental or moral development of under-18s must be subject to the strictest access control measures. In our guidance, we have interpreted this to mean that all VSP providers that have restricted material on their sites that is of a pornographic nature and/or unsuitable for a classification certificate should have a robust access control system that verifies age and prevents under-18s from accessing such material – see paragraphs 4.110 to 4.121 of the VSP guidance.

4.19   As outlined above, **UK Babe Channels** suggested that the introduction of age verification would be unaffordable for small VSP providers. As we set above at paragraph 3.185, we understand that small VSP providers which host pornographic material may incur additional costs associated with implementing age verification if they do not already have systems in place. We believe though that the age verification sector is mature and competitive enough to offer a range of solutions to adult VSPs. This view is supported by

publicly available unit pricing information from third-party providers[16], DCMS' impact assessment for the Online Safety Bill which cites age verification costs[17], regular engagement with age verification providers, as well as through their consultation responses. We are satisfied that adequate, easily integrated age verification options should be available. However, on the basis that these solutions are not affordable for smaller VSPs, we will consider the impact of this on smaller VSPs who suggest that their business may be significantly impacted as a result of age verification implementation. We will do this by working with smaller providers on the practical timelines for implementation of appropriate measures.

4.20   We note **UK Babe Channels**' concern that privacy concerns from their users may mean they visit alternative sites which do not have the same requirements. We consider that privacy concerns can be mitigated by consulting the ICO's guidance on UK GDPR requirements[18] and The Age Appropriate Design Code. We are working closely with the ICO through the Digital Cooperation Regulatory Forum (DRCF) and do not consider there is a conflict in the expectations of our respective regimes. There may also be options for VSP providers to use third party services which are privacy preserving and compliant with GDPR requirements.

4.21   We also note **UK Babe Channels**' concern that users concerns with using age verification systems may mean that they go elsewhere, which could have an impact on competition in the adult VSP sector. We consider the impact on user behaviour (in response to increased age verification) is uncertain. We accept though that the jurisdictional scope of VSP regulation may mean that users of adult UK-notified services may be inadvertently driven to use non-UK providers where they may not need to verify their age to access pornographic material. We are aware that there are a range of legislative steps being taken globally to protect children from the risks posed to them through pornographic sites, in particular through the harmonized framework of the AVMS Directive across Europe.

4.22   In addition, the forthcoming Online Safety Bill is expected to place new requirements on all services receivable to UK users. As we set out above, Ofcom will continue our close working with international regulators to share learning and understand their approaches to VSP, and wider online, regulation. We will aim to align approaches where we consider that this will deliver the greatest protection for UK users and promote compliance across industry.

4.23   We have made some changes to the impact assessment to make it clear that we have considered the potential impacts on VSP providers. This may be due to the cost of implementing age verification, the potential changes to user behaviour that results, and any commercial impact on the VSP provider.

---

[16] Example of the stated cost of £0.45 per age verification from provider VerifyMyAge. The provider Yoti has also issued a £0.25 per verification cost as part of it broader pricing strategy.
[17] The Online Safety Bill – Impact assessment
[18] Guide to the UK General Data Protection Regulation (UK GDPR)

4.24   We also recognise the view from **UK Babe Channels** that not all pornographic content is likely to have the same risk of harm to under-18s. This is explicitly recognised in the VSP Framework and Ofcom's guidance where we say that "restricted material that has the most potential to harm the physical, mental or moral development of under-18s must be subject to the strictest access control measures". As a result, we expect that the impact of protection measures required to protect against more 'extreme' adult content may be much more significant, but any impact will be proportionate to the potential for harm. VSP providers should have reference to BBFC age-based classification guidelines, which provide helpful information about the types of material that might be unsuitable for under-18s, by different age groups.

Specific impact on VSP providers that host pornographic content

4.25   One VSP provider asked why providers hosting pornographic content have been specifically targeted compared to platforms with other types of content which may cause harm when accessed by under-18s.

4.26   The legislative requirement is clear that material that has the most potential to harm under-18s is subject to the strictest access control measures. In our guidance, we have interpreted this to mean that VSP providers which specialise in pornographic material, VSP providers with services on which there is a significant risk of under-18s encountering pornographic material, and/or VSP providers that allow pornographic material in their terms of service should have robust age verification measures. This approach has been informed by our view that there is public expectation that restrictions around under-18s accessing pornographic material in the real world should also be reflected online;[19] the Government's response to the Online Harms White Paper,[20] which specifically references sites hosting online pornography as sites which will require a robust approach; and research which suggests that there is strong support from parents for age controls in relation to online pornography.[21] We also expect that VSP providers with non-pornographic material, but which is unsuitable for BBFC classification, to have in place a robust access control system that verifies age and prevents under-18s from accessing such material.[22]

Including freedom of expression/media literacy in the impact on creators.

4.27   The Government has already considered the impact on freedom of expression when introducing the legislation. The legislation aims to mitigate concerns in this area by requiring VSP providers to take into account the potential impact on the rights and legitimate interests of users when implementing appropriate measures, particularly those who engage with the service as uploaders and sharers of content.

4.28   Our guidance reiterates and emphasizes the importance of this, as reflected in the practicable and proportionate criteria in the Act. Therefore, our current approach in the

---

[19] This is consistent with our proposed guidance for on-demand programme services (ODPS).
[20] Full Government response to the Online Harms White Paper
[21] Consultation on guidance for VSP providers on measures to protect users from harmful material, paragraph 4.66
[22] See Guidance for VSP providers on measures to protect users from harmful material paragraphs 4.120-4.121

impact assessment is consistent with the approach and expectations in the legislation governing the VSP Regime, and therefore already takes account of the risk that legitimate content by creators is removed.

4.29   We also do not consider that there needs to be a specific reference to media literacy in the impact assessment. The guidance itself does not provide specific expectations on media literacy measures and we would expect any measures to be proportionate to the risk of harm.

A1. Conclusions on the impact of our VSP guidance

A1.1   In this section we set out our assessment of the likely impact of our VSP guidance. We assess the impact of those parts of our VSP guidance where we set specific expectations on VSP providers that we consider are central or strongly encouraged to adequately protect users.

Our VSP guidance stems from the regulatory requirements in the legislation

A1.2   The VSP Framework places an obligation on VSP providers to comply with the requirements in Part 4B of the Act. The expected costs that arise from the statutory requirements in the legislation have already been considered in the impact assessments produced by the European Commission when developing the AVMSD[23] and DCMS when transposing the directive into UK legislation;[24] as well as the Government's consultations on implementing the revised AVMSD and the provisions relating to VSP providers.[25]

A1.3   The guidance is designed to help VSP providers understand the statutory requirements and what is expected of them under the VSP Framework. In some places it sets out what platforms "should do" or "should consider" when implementing measures. These are not prescriptive requirements but intended as helpful suggestions to aid understanding of how compliance could be achieved.

A1.4   However, in some areas we have set specific expectations on VSP providers, where we consider it is unlikely that effective protection of users can be achieved without having this measure in place and it being implemented effectively. There are also areas where we strongly encourage certain approaches to effectively protect users.[26] These areas are as follows:

- **Terms and conditions about relevant harmful material**: VSP providers should have and effectively implement terms and conditions which prohibit the uploading of relevant harmful material.
- **Terms and conditions about restricted material**: Where a VSP provider has terms and conditions requiring uploaders to notify them if a video contains restricted material, it should take action in response to this notification which protects under-18s from that material.

---

[23] Impact Assessment for Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities
[24] Impact assessment for The Audiovisual Media Services Regulations 2020
[25] DCMS, Consultation: Audiovisual Media Services.
[26] See VSP guidance, page 2-3.

- **Flagging and reporting**: VSP providers should have and effectively implement a form of flagging and reporting mechanism.
- **Age verification systems**: VSP providers that have restricted material on their sites that is of a pornographic nature and/or material which is unsuitable for a classification certificate, should have a robust access control system that verifies age and prevents under-18s from accessing such material.
- **Risk management process**: VSP providers are strongly encouraged to implement some form of risk management framework to help providers understand the risk of harmful material on their platform and document the decisions they have taken when determining which measures are appropriate to protect users from harmful material.
- **Information collection and measuring effectiveness**: VSP providers are strongly encouraged to collect relevant information to measure the effectiveness of the measures for protecting users on their platforms.

A1.5   We do not consider that these proposed specific expectations on VSP providers are likely to result in material additional regulatory costs that exceed those previously estimated from the statutory requirement to comply with the VSP requirements in Part 4B of the Act, and which have already been considered in previous impact assessments.

A1.6   We do recognise, however, that the expectations on providers we have set out in our guidance to provide appropriate protection to users will have an impact on stakeholders. The following section considers these impacts.

A1.7   We have also now considered more explicitly the costs and benefits associated with the legal requirement to **Implement an impartial Dispute Resolution Procedure**. VSP providers are required to provide an impartial dispute resolution procedure for their users. We outline expectations for compliance with this obligation and the requirement for dispute resolution procedures to be impartial.[27]

Impact on stakeholders of the different expectations on providers outlined in our VSP guidance

A1.8   In the following paragraphs, we set out our assessment of the impact of our guidance on different stakeholders. This assessment has been informed by responses to our consultation and engagement with industry stakeholders. Below we outline the expected impact of the guidance on VSP providers, VSP users and advertisers.

What is the likely impact on VSP providers?

A1.9   The introduction of the VSP Regime and our guidance is likely to result in both positive and negative impacts on the VSP providers in scope of the regime. The guidance provides VSP providers with more clarity on what would be expected of them by Ofcom. This will allow

---

[27] See Section 5 of the VSP guidance

them to better plan their approach to protect all users from relevant harmful material and protect under-18s from restricted material.

A1.10   An additional potential positive impact for VSP providers is that compliance with the VSP Regime will assist services in preparing for compliance with the new online safety regime, given their shared objectives to hold services accountable for protecting their users through the adoption of appropriate systems and measures.

A1.11   We recognise that the VSP requirements and our guidance could also generate costs to providers. However, because the regime and our guidance provide flexibility for VSP providers on how they comply, we would expect that these costs should be proportionate to the benefits of the regime.

A1.12   Direct costs that VSP providers may incur from actions taken as a result of the guidance (and the regime more generally) could vary significantly, depending on the extent to which a VSP provider's existing approach is consistent with expectations under the regime. Broad categories of direct costs that could be incurred include:

a)   Costs associated with ensuring compliance are likely to be mainly staff or technological development costs. There are likely to be both one-off costs and ongoing costs for providers, including as the regime evolves over time and could include:

i)   Reviewing and assessing whether the measures they have in place are appropriate to protect users against the risk of harmful material;

ii)   Reviewing and assessing whether the measures they have in place meet the guidance principles for effective measures; and

iii) Where appropriate measures are not implemented, (or not implemented effectively), implementing measures so that they meet the guidance principles.

b)   Other regulatory costs include for example:

i)   Familiarisation with the statutory requirements of the VSP Framework;

ii)   Any fees payable to Ofcom for the running of the regime;

iii) Engaging with Ofcom through supervisory meetings, information gathering and responding to enforcement action.[28]

A1.13   We note that DCMS recognised there would be costs to businesses from the VSP Regime when developing the Statutory Framework for VSP providers but considered that these costs were justified.[29] DCMS also made it clear that these costs will depend on how in

---

[28] DCMS estimated the regulatory cost from Ofcom activities in setting up and monitoring the regime could be £18.8m over 5 years in PV terms. See DCMS impact assessment for The Audiovisual Media Services Regulation 2020

[29] DCMS indicated that the combined costs of the new regime could be ~£13m to VSP providers in jurisdiction in present value terms. This was based on estimates of the likely set-up costs for 8 VSP providers, including familiarisation with the regime and introduction of new measures where appropriate, and an estimate of ongoing costs based on an expectation that additional staff for content moderation would be needed to comply with the legislation. We note that the number of notified VSP providers is slightly higher than in DCMS' analysis. We anticipate therefore that if the analysis was re-run, total cost across all notified VSP providers would be higher than that estimated by DCMS. We expect though that the

practice Ofcom chooses to implement and enforce the VSP Regime through our guidance and enforcement powers. In drawing up this guidance, we have been mindful to ensure expected costs remain proportionate to the benefits of the regime.

Impact of the different expectations on providers in the guidance

A1.14   Overall, the VSP Framework affords VSP providers flexibility in how they protect their users. This reflects the diversity of the sector and the importance of technological innovation. However, as explained above there are some specific areas where we have outlined certain expectations on VSP providers because without them we believe it unlikely that users would be adequately protected.

A1.15   The impact of these potential activities on VSP providers will depend on VSP providers' existing approaches in these areas and whether they should revise these to ensure that they have taken appropriate measures to protect their users.

A1.16   We have considered the potential impact of these specific expectations in Tables 1 and 2 below.

Table 1: Measures which we consider are central to protect users

Measure	Potential impact on VSP providers	Expected benefits
Implementing and enforcing T&Cs related to relevant harmful material	Staff costs associated with reviewing and updating T&Cs to be consistent with VSP provider definitions of relevant harmful content and to satisfy the principles of transparency and ease of use as defined in the guidance. Staff and systems infrastructure costs associated with developing, maintaining, and improving moderation systems for relevant harmful material so it can be recognised and removed.	Our view is that this is necessary for any VSP provider to be able to protect its users. Appropriate and effectively enforced T&Cs are likely to discourage users from uploading content that they know is harmful, and improve recognition and removal of harmful material. Therefore, this could reduce the risk that users encounter it. (See paragraphs 4.24 to 4.58)
Uploader notifications of restricted material being actioned by the provider to protect under-18s	Development costs to upgrade systems and user interfaces to ensure appropriate functionality (incl. introducing	Our view is that a provider is likely to need to take action as a result of an uploader

incremental costs per notified VSP would be proportionate given the accompanied benefit that will be achieved by protecting users on these additional VSP providers.

	rating mechanisms, introducing access control measures for this content).	notifying a video containing restricted material. VSP providers taking action on identified content can protect users from encountering it, for example restricting access to under-18s (see paragraphs 4.17 to 4.23 of the guidance).
Effectively implementing a flagging and reporting mechanism	Development costs to upgrade systems and ongoing staff costs to review flagged content. However, we expect that many VSP providers will already have flagging and reporting mechanisms, so we expect costs are likely to be incremental in this area and mainly related to ongoing staff costs and ensuring that flagging and reporting systems remain fit-for-purpose.	Our view is that flagging and reporting tools are central to the protection of users. Effective flagging and reporting tools enable viewers to make a VSP aware of harmful content and take appropriate action. (See paragraphs 4.59 to 4.81).
Age verification systems for VSP providers that host restricted material of a pornographic nature and/or unsuitable for a classification certificate	Development costs to upgrade systems and user interfaces to ensure appropriate functionality, including potentially the integration of third-party age verification solutions. Costs associated with updates to T&Cs.	Our view is that the requirement to protect under-18s from the most harmful material means robust age verification measures are required for VSP providers with this type of material. (See paragraphs 4.108 to 4.121 of the guidance). There is increasing evidence on the feasibility and affordability of introducing age verification for VSP providers, including through third-party providers. This increases the potential for net benefits to arise from introducing age verification measures. (See

		paragraphs 4.18 to 4.26 above).

Table 2: Measures required by the VSP legislation

Measure	Potential impact on VSP providers	Expected benefits
Setting up of an impartial dispute resolution procedure	The legislation requires VSP providers to have an impartial dispute resolution procedure that relates to the taking and implementation of appropriate measures.[30] VSP providers who do not have an existing procedure will need to set one up, or adapt existing processes, to meet their legal obligations. VSP providers who do not already have this type of procedure are likely to incur costs from setting up impartial processes (e.g. separation of internal processes, or decisions made external to the VSP provider). However, we expect that providers would tailor their processes based on their own particular circumstances. This should therefore help to mitigate any costs. In addition to setting up the process, there is likely to be an ongoing cost for VSPs to administer this process. The impact on VSP providers is likely to depend on the number of complaints that they receive and which lead to dispute claims. The guidance recognises that there are ways in which a provider may	Users will benefit from an ability to enter a dispute resolution process concerning decisions made by VSP providers in relation to the taking or implementing of measures in Schedule 15A. Greater understanding of VSP decision making processes will also give users more confidence in using individual platforms. VSP providers themselves will also benefit if the dispute resolution process increases feedback and transparency of a VSP provider's internal decision making. The dispute resolution procedure can also help ensure moderation and enforcement decisions are consistent and fair for users when the dispute relates to the implementation of terms and conditions.

---

[30] See Section 5 of the VSP guidance

| | be able to manage dispute numbers by investigating methods to filter frivolous and/or vexatious complaints, or by requiring that a user exhausts a complaints process first. | |

Table 2: Measures strongly encouraged to support compliance

Measure	Potential impact on VSP providers	Expected benefits
Risk management process	Staff costs to develop, manage and embed risk management processes on an ongoing basis. Research activities to understand the risk of harm on the platform based on individual platform characteristics. Risk prioritisation discussions by senior staff members. Developing a risk management plan with key risk indicators. Recording and documenting the risk management process. Interactions with Ofcom to describe any risk management approach that has been taken.	Our view is that embedding a culture of identifying, assessing, planning for and managing any risks and monitoring to ensure that risks are appropriately mitigated will help to support decisions about which measures are appropriate for protecting users and how to implement them adequately. (See paragraphs 7.26 to 7.49). A comprehensive risk management approach is also likely to be the most effective way by which a VSP provider can satisfy itself that it is complying with its obligations under the regime so that they protect users from harm on their platform. (See paragraph 7.30). We note that assessment and management of risk will likely form part of the forthcoming online harms regime and is also part of the European Commission's Proposal for the Digital Services Act.
Information collection and measuring effectiveness	Staff costs to determine information that can indicate effectiveness of the measures. Staff and systems infrastructure costs associated with collecting	Understanding the effectiveness of measures is vital for platforms to understand how well they are working to protect users from

	and analysing information on those measures on an ongoing basis.	harmful content. (See paragraph 7.50 of the guidance). The collection of data and information would form an important aspect of this as it will help the provider to satisfy itself that it is complying with its obligations under the regime.

A1.17   Our view is that any material costs in these areas are likely to be proportionate given the expected benefits that are identified.

A1.18   The introduction of appropriate measures can also lead to user frictions, which may decrease the number of users of a particular VSP platform or decrease the time each user spends on the platform. As outlined in paragraphs A1.29 to A1.32 below this may impact the competitive environment in which a VSP provider operates and so there could be some negative commercial consequences to individual VSP providers. However, implicit in the framework of the VSP Regime is that because it affords flexibility to providers, any negative impacts will be proportionate to the level of harm which the measures are protecting against.

What is the likely impact on other stakeholders?

A1.19   The implementation of the VSP Regime and changes made by VSP providers (as a result of our guidance) are likely to result in both positive and negative impacts on non-VSP stakeholders. These potential impacts are summarised for different stakeholders below.

VSP users (viewers)

A1.20   The main beneficiaries of the actions VSP providers may take based on our guidance, will likely be users accessing VSP services. This is because by following the guidance platforms will be better equipped to understand the requirements of the VSP Framework and the measures that may be appropriate for them to take to protect users of VSP services from potentially harmful material. For example, effective implementation of appropriate measures should, over time, reduce the prevalence of harmful content, or the risk of users encountering it.

A1.21   However, there may be some negative effects from the introduction of the new regime. For example, VSP viewers may need time to familiarise themselves with any changes to protection measures that VSP providers implement. Adult viewers may also find it more difficult or time consuming to access restricted material. They may also have privacy concerns if they are required to provide personal details to VSP providers. We consider that these privacy concerns should however be mitigated because providers will need to have regard to data protection law requirements.

A1.22   Balancing these two factors, we consider the net benefits from our guidance to viewers of VSP content will likely be positive.

VSP users (creators)

A1.23   The response of VSP providers to the guidance will have knock-on effects on VSP users who create and upload content. There is the potential for additional protection measures to increase the risk of unnecessary removal of legitimate content if those measures are implemented overzealously. Our guidance aims to mitigate against this by setting in context the requirement for VSP providers to take into account the potential impact on the rights and legitimate interests of users, particularly those who engage with the service as uploaders and sharers of content.

A1.24   If additional protection measures put in place by VSP providers impact the number of viewers and/or time spent by viewers on the platforms, then this could also affect the commercial opportunities for users who create content. For example, overall viewership may go up if VSP viewers are attracted by a safer VSP environment and so this could have a positive impact for some VSP creators that focus on child-friendly content. In particular, they may be able to attract greater viewing figures for their individual pieces of content and therefore receive increased revenue from subscriptions or a share of advertising revenues.

A1.25   However, we also recognise that viewership numbers could reduce for some VSP creators because viewers may perceive some protection measures as time-consuming barriers to access VSP content.[31] This could therefore limit legitimate commercial opportunities for creators on the platform. Negative impacts for users should nonetheless be mitigated because when considering the proportionality of any particular measures, VSP providers must take into account the interests of users such as uploaders and sharers of content.

A1.26   We also note that most VSP creators are also likely to be viewers and will therefore also receive the positive impacts from the regime to VSP viewers.

VSP advertisers

A1.27   There are potentially significant benefits to advertisers from the introduction of the guidance. Specifically, we expect advertisers will have more confidence to place adverts on VSP platforms due to a lower risk of being associated with harmful content.[32] This is likely to increase brand trust and reduce the risk of a brand being significantly tarnished from individual incidents where an advertiser is associated with a particularly harmful piece of content.

A1.28   There is also likely to be a consequential impact on advertisers from any changes to VSP viewer numbers from the introduction or modification of protection measures that arise

---

[31] For example, some protection measures may increase the time required to access VSP content and may require a viewer to provide greater amounts of personal information.

[32] A number of brands have previously been concerned with being associated with harmful content via programmatic advertising. For example, https://www.thetimes.co.uk/article/big-brands-fund-terror-knnxfgb98

from the guidance. As described above this could be positive or negative depending on whether safer platforms attract new viewers, platforms become 'safer' for advertisers due to less brand risk, or whether viewer numbers decrease. However, some of these financial effects may be muted for advertisers themselves as advertising fees to VSP platforms would be expected to adjust depending on the number of viewers that see them. For example, if a lower number of VSP viewers are exposed to an advert, we would expect any payment the advertiser makes to the VSP provider would also be reduced. This would limit the overall impact on the advertiser.

Other impacts

A1.29   There is some probability that VSP providers will pass on any increase in their costs to other stakeholders, either through higher advertising prices, more advertising or higher subscription fees.

A1.30   Another potential impact from the guidance could be the effect on the competitive environment for VSP providers. Smaller VSP providers without sufficient scale may not be able to meet the expectations required by the guidance. This could potentially have a detrimental impact on the competition in the market for VSP services as it could reduce the opportunity for smaller VSP providers to enter the market and compete with larger and more established VSP providers. It may also mean that more established VSP providers cannot meet the expectations in the guidance and remain commercially viable. Any reduction in competition would likely have an impact on innovation in the VSP sector. We also recognise that innovation may be affected by other factors, including potentially the impact on innovation from additional protection measures that could make it more costly to introduce new products or features.

A1.31   There is also the potential for VSP providers subject to UK jurisdiction to lose market share to VSP providers in other jurisdictions if regulatory expectations elsewhere are significantly lower. As a result, they may experience a loss of revenue as viewership on their platform is reduced. In response to this, one impact could be that existing UK-based VSP providers choose to move their headquarters to other jurisdictions or new VSP providers may set-up in other countries if they consider the costs of complying with the UK VSP Regime is too onerous. This could therefore lead to knock-on impacts on UK tax revenues and UK employment. Further, if VSP users can easily access content from overseas-based VSP providers there is the potential for the effectiveness of the regime to be diminished.

A1.32   As noted above at paragraph A1.13, DCMS recognised there would be costs to businesses from the VSP Regime when developing the Statutory Framework. The framework requires VSP providers to take measures proportionate to the risk of harm their platform poses to users. Implicit in this framework is that if VSP providers cannot meet their regulatory obligations and remain commercially viable, then this cost is justified by the benefit to protect users. However, we consider these potential negative effects are likely to be limited because:

a) Proportionality is an integral part of the guidance, and how measures are implemented, which mitigates the potential for significant negative impacts of this type.

b) The VSP Framework in the UK transposes the Audiovisual Media Services Directive, which all EU Members States are also required to implement. The UK adhered to the minimum requirements of the Directive, however, other jurisdictions may choose to go beyond the requirements of the Directive. This means in practice the opportunity to move to jurisdictions in Europe with lower regulatory expectations is likely to be limited. We are also continuing to work with other national regulatory authorities towards a consistent application of the Directive.

c) The forthcoming Online Safety Bill will bring all VSP providers with UK users into UK jurisdiction. This may mean that any advantage that would come from a VSP provider relocating would only provide short-term benefits.

Conclusions on the impact of our different expectations on providers in the guidance

A1.33 Where we set specific expectations on VSP providers in the guidance, we consider they are either central to protecting users or we strongly encourage their adoption for this purpose. On the basis of the assessment above, our view is that the costs implied are justified by the benefits they seek to generate in terms of protecting users from harm.

A1.34 We do not consider that our guidance should entail any material additional regulatory costs for VSP providers above those that result from the statutory requirement to comply with the VSP requirements in Part 4B of the Act and which have already been considered in previous impact assessments.

A1.35 Therefore, we consider that the identified costs that may arise from our specific expectations in the VSP guidance, as described in the previous section, do not materially impact stakeholders in a way that is disproportionate to the benefits that are likely to be secured from them.