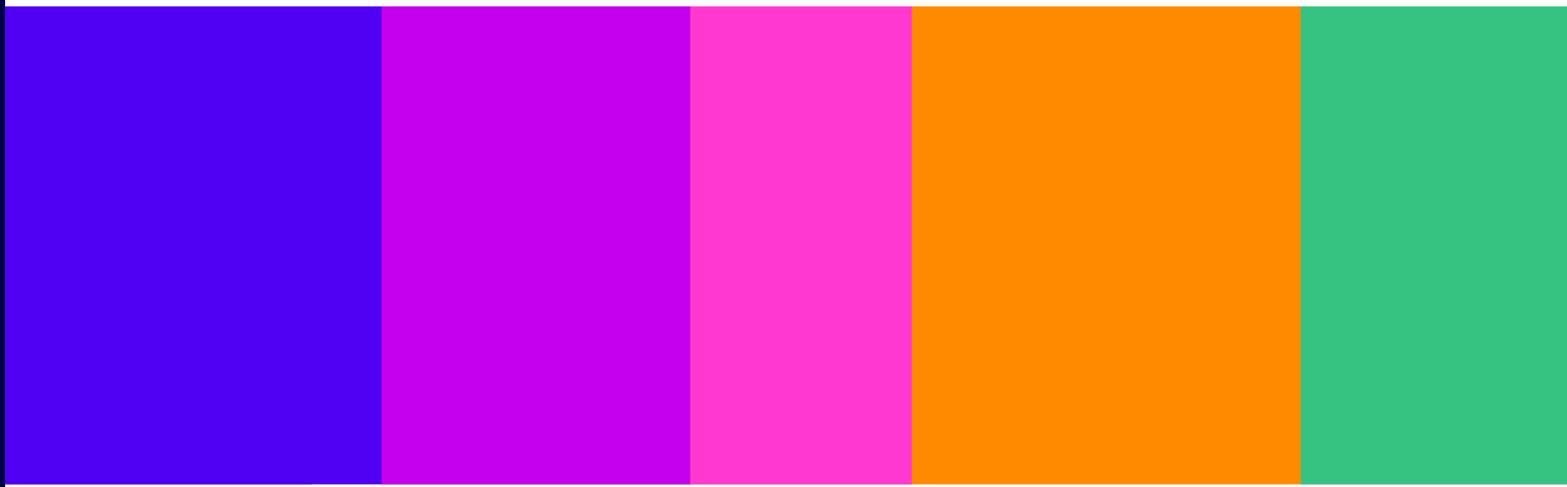


Regulating Video-Sharing Platforms (VSPs)

Our updated plan and approach

VSP Report

Published 25 January 2024



Contents

Section

Overview	3
How we have regulated VSPs	5
Our updated VSP priorities	14

Annex

A1	Background	19
A2	Comparison of VSP and online safety regimes	22

Overview

Ofcom is the United Kingdom's (UK) communications regulator, overseeing sectors including fixed-line and mobile telecoms, the airwaves on which wireless devices operate, post and TV and radio broadcasting. We have regulated video-sharing platforms (VSPs) since November 2020 and were formally appointed as the online safety regulator in October 2023.

The VSP regime came into force in November 2020 and Ofcom launched our [VSP Guidance](#) for providers and [Plan and Approach](#) in October 2021. During our [first year](#), we found that while all VSPs had some safety measures to protect users, there was room for improvement. Since then, we've taken a broader look at the way platforms set, enforce, and test their approach to user safety – including looking at [VSPs' user policies](#) and [how VSPs protect children](#) from encountering harm.

This report summarises how we have regulated VSPs so far. We also set out our priorities for the rest of the time the VSP regime is in force – before it is replaced by the online safety regime.

We've focused on improving safety measures for users

The VSP regime requires VSP providers to take and implement safety measures that are appropriate to protect users from certain types of harmful and/or illegal videos online. The VSP legislation lists some measures that VSP providers can take, including:

- having - and effectively implementing - clear and comprehensive **terms of service**,
- having effective and easy-to-use **user reporting, flagging, and complaints functionalities**, and
- applying appropriate access controls to protect children, like **age assurance** and/or **parental control measures**.

It's for VSP providers to decide what safety measures they take, but they must ensure these measures work well in practice to protect users. Our VSP Guidance explains this in more detail. Ofcom's role as VSP regulator is to ensure services meet their duties to protect users. We assess the effectiveness of safety measures implemented by VSPs and consider whether they are - in practice - working effectively to protect users. Where we find concerns, we seek improvements.

VSP providers are not required to completely eradicate harmful or illegal content. Their focus instead should be on ensuring their safety measures operate to remove as much harmful or illegal content as possible - and as quickly as possible. In turn, we don't adjudicate on individual pieces of content, and instead focus on getting to the heart of any online safety risks. Where we find them, we ultimately look to push improvements in platforms' safety measures to protect UK users from harm.

We've used a mix of regulatory tools to push for positive change

Since the VSP regime has been in force, we've used our range of regulatory tools to influence positive changes in VSPs' safety measures. These tools are not necessarily mutually exclusive and often are used in conjunction with each other to achieve the best outcome. We set out some highlights below:

- **Supervision:** Supervision involves building productive relationships with our notified platforms through regular engagement. We use supervision to learn about safety measures, pre-empt risks to users, and push for improvements to user safety. For example, we've worked with OnlyFans to secure changes to its reporting functionalities so that serious harm can be

prioritised quickly. Last year, OnlyFans also introduced additional measures to verify the age of UK subscribers in response to VSP regulation.

- **Enforcement:** We have wide-ranging tools at our disposal to take enforcement action where we have compliance concerns, to hold platforms to account and to rectify poor conduct. For example, we've concluded an investigation about [Tapnet's](#) failure to provide information as required and opened further investigations. We have also used alternative compliance tools to respond to concerns. For example, our sector-wide enforcement programme into [age assurance on adult VSPs](#) has resulted in tangible positive improvements, including the introduction of age assurance measures on adult platforms [RevealMe](#) and [AdmireMe](#). We also secured important commitments from [BitChute](#) to improve its safety measures.
- **Transparency:** We can publish reports about the measures taken by platforms and how they have been implemented to protect users from videos containing harmful material. Publishing VSP reports helps us to empower the public, hold platforms accountable, and drive improvements by showcasing good industry practice. For example, our [report on user policies](#) led to positive commitments from VSPs to improve their terms and conditions and make them more readable and digestible (which we'll follow up on).

Alongside using the above regulatory tools, we've engaged extensively on a national and international scale, including with civil society, global networks, and other EU VSP regulators.

We've set our big priorities for the remainder of the VSP regime

We have had four broad aims in place since the start of the VSP regime: **to raise standards, address non-compliance, increase transparency, and get ready for the future online safety regime**. These will remain constant throughout the rest of the VSP regime. Taking what we've learnt so far and the areas where we can have the greatest impact, we've identified our big priorities for the remainder of the VSP regime. We'll prioritise making sure that:

1. **there are clear user policies in place that are easy to find and understand,**
2. **terrorist videos or videos that incite hatred and/or violence are taken down quickly,**
3. **child abusers are prevented from sharing and/or watching child sexual abuse videos,**
4. **children are prevented from finding and viewing pornographic videos on adult platforms,**
5. **children are protected from finding and viewing other age-inappropriate videos, and**
6. **all users can access easy-to-use and effective tools to report content or submit complaints.**

Within these priorities, we expect to focus predominantly on areas that will remain relevant under the broader [online safety regime](#). That said, the VSP regime continues to be a priority for Ofcom – it allows us to improve safety for VSP users ahead of the full force of the online safety regime.

The online safety regime will eventually replace the VSP regime

The VSP regime has been – and continues to be – an effective test bed for how online safety regulation works in practice and is key to helping us prepare for the new [online safety regime](#). The Online Safety Act 2023 received Royal Assent in October 2023. However, the VSP regime remains a live regulatory regime until such time as the VSP legislation is repealed by the UK Government. We'll support platforms regulated under the VSP regime through the transition from the VSP regime to the online safety regime.

How we have regulated VSPs

This section outlines how the VSP regime operates, and how we have approached regulating VSPs to ensure their safety measures operate to effectively protect users from harmful material.

The VSP regime is focused on improving safety measures, not on assessing content

Ofcom has regulated VSPs based in the UK since November 2020

The VSP Regime is set out in Part 4B of the Communications Act 2003 (the Act). The requirements for platforms came into effect in November 2020. At the same time, Ofcom was appointed as the regulator for VSPs that have the required connection with the UK.

Briefly stated, VSP providers are required to take and implement such safety measures as are appropriate to protect users from videos containing harmful content. You can read more about the regulatory requirements, the harmful material in scope of the VSP regime, and the measures VSPs must consider taking in the [VSP Guidance](#).

More detail on the background of the VSP regime can be found in Annex 1.

UK online regulation is focused on platforms' safety measures

The VSP regime – and the broader online safety regime¹ - are both focused on online platforms having effective safety measures in place to protect their users from harm.

The phrase 'safety measures' capture a wide range of activity that services use to keep users safe. For example, **user reporting** is a process by which users can flag specific kinds of harmful content to a platform which can then help platforms in prioritising review of the highest harm content. Another example is **content moderation**,² whereby platforms review potentially harmful content (often through a combination of human moderators and technology) and take down content that breaches their community guidelines.

Under both UK online safety regimes, platforms are not obliged to consider whether individual pieces of content are appropriate or allowed on their platform. This type of content-based regulation would likely be impractical due to the scale of online content shared every day. By focusing on the effectiveness and broader impact of their safety measures and process, platforms can achieve wider systemic change and increased safety to users. For example, making sure they have the right systems and resources in place to deal with user reports quickly and effectively.

Our role is to improve platforms' safety measures

Our role as VSP regulator, and now as online safety regulator, is to ensure services meet their duties to protect the general public from harmful content online.³ We must also balance this with ensuring

¹ See: [Approach to Implementing the Online Safety Act](#)

² Ofcom has recently [published a report on content moderation practices within user-to-user services](#).

³ In exercising our functions under both regimes, we also have an overarching duty to further the interests of citizens and consumers.

our approach to regulation upholds the importance of fundamental rights, in particular the rights to freedom of expression and privacy.⁴

Given how UK online regulation has been established in legislation, Ofcom's role as online regulator consequently centres on tackling the root causes of illegal and harmful online content, by considering the effectiveness of platforms' safety measures. We do not have any specific powers to regulate individual pieces of content.

Our focus is therefore on assessing the effectiveness of services' safety measures and pushing positive changes to further protect users. By seeking improvements to services' safety measures, we will reduce risk at scale, rather than focusing on individual instances of harmful content. This supports an evidence-based, proportionate approach to online regulation and avoids any consequential unintended impact on users' right to freedom of expression.

Our experience in regulating VSP content continues to help us to prepare for our additional expanded responsibilities under the Online Safety Act. We see VSP regulation as an opportunity for VSPs to change so that trust and safety are embedded into their service design from the very beginning, which will set them up for the online safety regime.

This section below explains more about how regulation has worked under the VSP regime, including case study examples to illustrate our approach.

How we're improving VSPs' safety measures

At the start of the VSP regime in October 2021, we set out Ofcom's approach to regulating VSP providers and initial plan of work in our [Plan and Approach document](#). This laid out our four broad aims: **to raise standards, address non-compliance, increase transparency, and get industry and ourselves ready for the future online safety regime.**

In our first year of regulation, we worked to build a comprehensive baseline knowledge of the VSP sector, which led to publishing our [report on the first full year of VSP regulation](#). This document laid out our findings from Ofcom's first full year of regulating VSPs. It also set out our aim to more broadly look at how platforms set, enforce, and test their approach to user safety, with a specific focus on:

- ensuring VSPs have sufficient processes in place for setting and revising comprehensive terms and conditions (generally known as Community Guidelines) that cover all relevant harms,
- checking that VSPs apply and enforce their Community Guidelines consistently and effectively to ensure harmful content is tackled in practice,
- reviewing the tools VSPs provide to allow users to control their experience and promote greater engagement with these measures, and
- driving forward the implementation of robust age assurance to protect children from the most harmful online content (including pornography).

To tackle these priorities, we've used a wide range of our regulatory levers to push for improved safety for VSPs' users – including policy, supervision, enforcement, transparency, and international engagement. We discuss these further below.

⁴ As a public body, Ofcom must act compatibly with the European Convention on Human Rights.

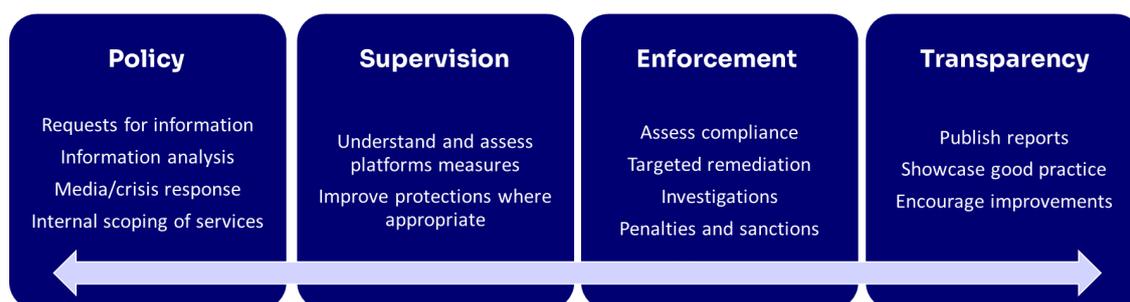
How we have used our regulatory tools

All our regulatory activity is focused on improving VSPs' safety measures to ensure users are protected. It can be broadly broken down into four functions – **policy development, supervision, enforcement, and transparency**.

In running the VSP regime, we gather and analyse information from a range of sources, which are then triaged and analysed and help us build a picture of potential compliance concerns. We deal with these incoming issues effectively, promptly, and proportionately through our regulatory tools to ensure that VSPs are taking appropriate measures to protect their users from harmful material.

We describe our four core functions in more detail below:

- **policy development** to complete analysis across one or more VSP(s) to better understand harms, safety measures, and establish what is good or poor practice,
- **supervision** to build effective, trusted relationships and push for changes within services to understand, assess and improve their protection measures,
- **enforcement** action to drive targeted improved outcomes, hold services to account, and incentivise broader compliance, and
- **transparency** to shine a light on good or poor practices, empower users to choose safer services, and secure higher standards.



These tools are not necessarily mutually exclusive, and we often use them in conjunction with each other. In the following section, we set out several case studies from our experience regulating VSPs, highlighting how our work has incentivised platforms to make changes to their systems and processes to improve user safety.

In addition to these tools, we engage extensively with a broad range of relevant stakeholders, including our international counterparts.

Policy development

Effective policy development and analysis underpins all our regulatory activities. We carry out policy development to establish the nature of services, understand different platforms' safety measures and risk of harm, and undertake analysis across VSPs to help identify what might be good or poor practice. This work directly informs our supervision and transparency activities, as well as identifying potential compliance issues that may be passed to our enforcement team.

Our policy development work often involves consideration of information from sources including responses to information requests, desktop research, VSP complaints data analysis, and horizon-

scanning. We don't generally assess individual pieces of content,⁵ but instead focus on what the available evidence tells us about the measures that have been taken and their efficacy.

Importantly, we'll analyse the information received to consider what are examples of good and poor practice when it comes to VSP safety measures – and what action might be needed to drive improved outcomes. For example, last year, we sent out requests for information about VSPs' safety measures (including on user policies and child safety measures), and this information has been incorporated into our recently published VSP transparency reports (described below).

Assessing the effectiveness of measures is an important part of our work, and we are continuing to learn about what metrics and measures are useful in this respect. For example, [the work](#) we are doing within the World Economic Forum (WEF) seeks to assess how platforms should approach digital safety risks and measure the impact of their interventions.

Taken in full, policy development represents a broad suite of activities that allow us to better understand the platforms we regulate and what needs to be improved within their systems and processes to address user harm.

Supervision

The term 'supervision' describes a set of activities we undertake to manage Ofcom's relationships with services to understand and mitigate future risks and secure improvements to VSPs' safety measures. This includes building trusted productive relationships through regular engagement. In line with our approach described above, our supervision activity focuses on the effectiveness of VSPs' safety measures in protecting their users, not on individual pieces of content.

We have continued to develop our supervisory approach over the past year within the VSP regime, ahead of our duties in the online safety regime. Supervision generally encompasses proactive engagement with priority services, and reactive engagement with other services as and when needed. Under the VSP regime, we focus most of our supervision resources on the highest reach and highest risk services – in other words, those services that are likely to have the greatest impact on users' safety. Alongside this, we continue broad monitoring across all VSPs.

Ultimately this allows us to:

- understand the nature of risk of harms on those services and the systems and processes that are already in place to tackle them,
- assess the effectiveness of their safety measures, considering the specific circumstances of the individual service (including its risk levels, size, and capacity), and
- where appropriate, work with the service to secure improvements in those measures as quickly and efficiently as possible.

We've successfully established our supervision function over the past year and have received positive engagement from the services we have prioritised. We've been able to use these relationships to learn more about safety measures and push for improvements where appropriate.

⁵ Allegations of harmful content being present or widely available on a platform may act as a trigger or indicator for Ofcom to consider whether there are compliance concerns.

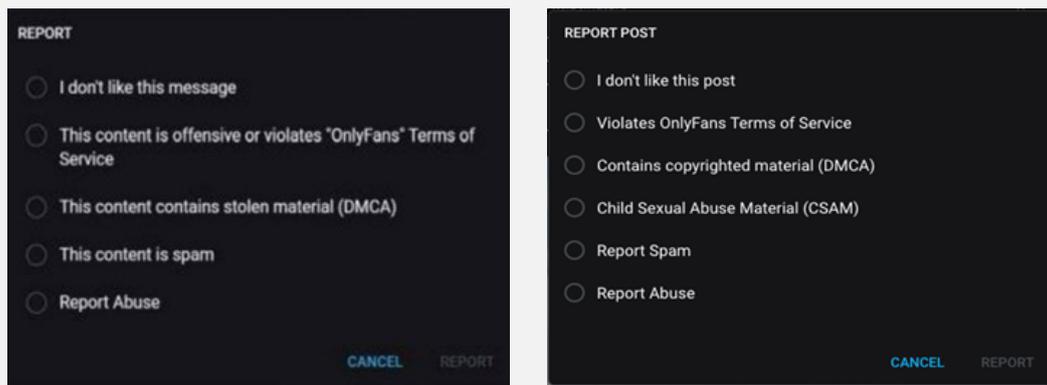
Case study: OnlyFans

OnlyFans is a notified VSP generally known for hosting adult content. OnlyFans' platform allows users to report illegal/harmful videos to OnlyFans for further review. This functionality originally offered five categories for users to submit their reports against (see below). Non-users can report any suspicious content/accounts via email.

Ofcom was keen to understand how OnlyFans prioritised user reports relating to suspected CSAM without having a specific CSAM reporting category. OnlyFans explained that they review every report and prioritise them according to their substance, regardless of which reporting button a user chose, but did not have a specific category for reporting CSAM material. During our regular supervisory engagement with the service, we drew their attention to the Canadian Centre for Child Protection's [2020 report](#) which argued that not having a specific reporting category for CSAM made it harder for services to prioritise CSAM reports and collect CSAM reporting data.⁶ Ofcom's own research and subsequent policy development also found that user reporting systems with granular and specific reporting categories are generally easier.⁷

We engaged with OnlyFans and suggested they consider expanding their reporting categories, to make it easier for users to report CSAM and for OnlyFans to prioritise those reports appropriately. OnlyFans considered the evidence we presented and, voluntarily within three months, changed their reporting tool to add a specific category for CSAM (see below). OnlyFans is working with Ofcom to monitor the impact of this change and to gain a better understanding of how reporting categories can be made most effective.

OnlyFans' old vs new reporting categories



Our work with OnlyFans demonstrates how supervision works in practice – using trusted relationships and open conversations to secure agile solutions and embed good practice. Although the impact and effectiveness of this change to OnlyFans' platform is still yet to be fully assessed, it's

⁶ Canadian Centre for Child Protection, 2020. [Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms](#), page 7.

⁷ https://www.ofcom.org.uk/data/assets/pdf_file/0020/241832/Online-Trials-Appendix-2-Reporting-Mechanisms.pdf

important that Ofcom and services can work collaboratively and move quickly to make changes to better protect user safety.

Building effective relationships has also meant we can flag concerns quickly when they arise. For example, when news of the crisis in Israel and Gaza broke out in October 2023, we sent an [open letter](#) to VSPs about the increased risk of their users encountering harmful content stemming from the crisis, and the need to protect users from such content. We were able to quickly engage with platforms to understand the steps they were taking to respond to the crisis and protect users from harmful material.

Enforcement

We've undertaken a wide programme of enforcement activity since we started regulating VSPs, seeking positive changes and addressing poor compliance. The focus of our enforcement activity is primarily to secure improvements in VSPs' systems and processes to improve user safety on a broad scale, but it may also be appropriate to punish poor behaviour or incentivise wider compliance across the industry.

Where we suspect that a VSP has not complied with its duties under the VSP regime, we have a wide range of powers and tools at our disposal. **These are outlined in more detail in Annex 1.** We make an assessment of which tools are most appropriate in any given case in line with our [enforcement guidelines](#).

Where there are reasonable grounds to suspect non-compliance and we decide to use a formal enforcement approach to resolve our concerns, we may open an investigation. However, we'll typically engage with a platform first about our concerns before considering using our more formal tools. Examples of our **formal enforcement activity** include:

- Completing an [investigation into Tapnet](#) and imposing a financial penalty of £2,000 for failure to respond to an information request and failure to co-operate fully with Ofcom.
- An [investigation into Secure Live Media Ltd](#) (believed to be provider of adult platform, CamSoda) to assess whether they were providing a notifiable VSP and measures in place to protect children).
- An [investigation into My Medial World Ltd](#), provider of OneVSP, to consider the measures it has in place to protect its users from harmful material.
- An [investigation into TikTok](#) to consider whether it failed to comply with its duties to provide information in response to an request for information in relation to Ofcom's recent VSP report on how VSPs stop children encountering harm.

In other cases, we have entered periods of compliance remediation, where we have agreed improvement plans with certain platforms in lieu of opening formal investigations, setting clear targets for improvement against an agreed timescale. Examples of **compliance remediation**:

- Further to our [enforcement programme](#) opened to better understand age assurance measures on UK established adult VSPs (see box below), we have secured improvements on age assurance measures on adult platforms, including:
- measures recently implemented by [Tapnet Ltd](#) to protect under-18s from pornographic videos on RevealMe,
- commitments from Kiwi Leisure Ltd to introduce age assurance measures on its AdmireMe platform so that under-18s are protected from pornographic videos, and
- positive engagement from other notified VSPs who are in the process of making similar improvements, which we will share details of in due course.

Following concerns raised after the shooting in Buffalo, New York in May 2022, we [engaged with BitChute](#) to learn more about its systems and processes. Following Ofcom's engagement, BitChute has committed to making important changes to protect users from harmful material including (i) increasing the coverage and capacity of its moderation team, (ii) extending user reporting to non-registered users, and (iii) collecting additional metrics to measure the impact of the changes it has made.

Case study: Small adult platforms

On 10 January 2023, Ofcom opened an enforcement programme to look at whether UK-established VSPs that specialise in adult content have appropriate age assurance measures in place. We have considered the measures that platforms have taken to get assurance as to the age of their users and prevent under-18s from watching pornographic videos.

Following a period of detailed information gathering and analysis, we were concerned that some platforms were not effectively protecting underage users from pornographic content available on these platforms. This included the VSP, RevealMe, operated by Tapnet, amongst a few others. In lieu of opening a formal investigation, we gave them a short period to make changes to bring themselves into compliance.

In response to our work, RevealMe has made significant changes to its access control and age assurance measures. Under its improved processes, Tapnet can obtain robust assurance as to the age of RevealMe's users by requiring them to verify their age when entering the site or to sign into a registered account in respect of which their age has already been identified. Users can verify their age by either submitting validation to a third-party automated age verification tool, or by using a credit card to pay. Of note is that Tapnet put in place an interim age verification measure while this process was being developed and tested to meet our required timeframe for improvements.

The relationship with Tapnet is just one example of how we can work positively to achieve better online protections for users. We will continue to work constructively with regulated VSPs to drive compliance and secure better outcomes for consumers and use enforcement where necessary.

Transparency

Under the VSP regime, Ofcom has the power to publish reports about the measures taken by platforms for the purposes of protecting users from videos containing harmful material and the ways in which such measures are implemented.⁸ Publishing VSP reports helps inform and empower the public⁹, hold platforms accountable, and drive improvements by showcasing good practice across the industry. This is also an opportunity for Ofcom to be transparent about the work it has

⁸ Please refer to section 368Z11(1)(b) of the Communications Act 2003.

⁹ As we noted in our 2023 [Journal of Online Trust and Safety](#) article, 'the public' could include several interested parties, such as prospective or actual users of the service but also other interested stakeholders. (For examples, suppliers of services to the platform (such as payment providers), advertisers, investors, third-sector organisations, journalists, and researchers).

undertaken within its policy, supervision, and enforcement functions. We aim to make our reports accessible and engaging for our readers.

We've trialled different approaches to transparency reporting under the VSP regime. In 2022, we published [one comprehensive report](#) on what we'd found during our first full year of VSP regulation, including annexes setting out platform-specific reports for each of the notified VSPs. Since then, we've focused on publishing shorter, thematic transparency reports:

- **What we've learnt about VSPs' user policies (published in August 2023):** This [report](#) looked at the challenges VSP providers face when implementing their terms and conditions and set out to provide greater transparency for the public on user policies. The report considered the different approaches VSPs are currently using to implement their terms and conditions and highlighted examples of what we deem to be good practice.
- **Protecting children from accessing potentially harmful content (published 14 December 2023):** The [report](#) focused on Twitch, TikTok and Snap and looked at the measures these VSPs are using to prevent children from encountering harm. We noted that all three use self-declaration to understand user ages and tailor their experience, and that this is easy to bypass. This will be an area of focus for our engagement going forward.

We also aim for our reports to encourage platforms to engage with what Ofcom considers to be good practice and consider making changes to their systems and processes. They can form the basis of supervisory discussions and help providers understand where they can make positive changes. For example, following publication of our [VSP report on user policies](#), various VSPs committed to improve their terms and conditions and make them more readable and digestible.

International collaboration

Although the VSP regime only applies to services with the required connection with the UK, we recognise that VSPs are global in nature. Facilitating international regulatory collaboration helps us secure better protections for users and to further our respective domestic objectives. It is also helpful for the services that we regulate, and enabling collaboration around regulatory expectations and supervisory approaches can promote services' compliance across jurisdictions. Our international engagement has played an important role in achieving our objectives to date. Our recent [blog](#) summarised our international collaboration in detail.

In early 2023, we joined forces with other VSP regulators in Belgium, Cyprus, France, and Germany to create the International Working Group on Age Verification (IWGAV), the only dedicated forum for VSP regulators to exchange information and best practices around their approaches to age assurance. In March 2023 the working group published a joint statement and has since doubled its membership, creating a critical platform for regulators to share research and expertise on emerging, innovative, and novel methods of assessing the age of users to keep children safe. This international alignment on the policy priority of protecting children from accessing pornographic material on VSPs helps to create joined up collaborative approaches to online safety regulation and ultimately protect users' safety online.

The IWGAV is just one case-in-point of the importance of international engagement to achieve our VSP objectives. For example, in September 2023, we made a [formal submission](#) to a public consultation by our Irish counterparts, Coimisiún na Meán, to support it in developing its upcoming rules for Irish-based VSPs.

We also meet routinely with VSP regulatory counterparts on a range of specific issues, from jurisdictional matters to regulatory implementation, to supervision. We've recently co-founded the

[Global Online Safety Regulator Network](#), the only global forum dedicated to supporting collaboration between online safety regulators and are pleased to be taking on the role as Chair this year.

International VSP engagement will remain a critical priority, especially as it complements our work on delivering the international objectives of the new Online Safety Act. Crucially, our engagement internationally extends beyond fellow regulators, and we seek to build trust and understanding with the broader community of VSP policy stakeholders. Many services we will regulate under online safety regime will operate across, and have regulatory duties in, other jurisdictions. The VSP framework continues to offer the opportunity of significant learnings not only for us, but for the international community as we all work together to make lives safer online.

VSP sets the foundation for the online safety regime

As set out in our [Approach to Online Safety](#) publication, the VSP regime is an effective testbed for how online safety regulation can work in practice. By using the range of regulatory tools available to us, we have been able to make great progress in:

- identifying, researching, and providing analysis of what is good and poor practice,
- recommending changes and embedding standards through supervisory engagement,
- improving measures by taking proportionate enforcement action when we have identified areas of concern, and
- shining a light on good and poor practices via transparency reporting.

We'll continue to push for better user protections under the VSP regime. This will help orient our programme of work on online safety and serve as the building blocks to our approach - emphasising the importance of evidence-based, iterative, and proportionate responses from us as the regulator.

Annex 2 sets out more information about the differences between the two regimes.

Our updated VSP priorities

In this section, we set out our refreshed priorities for the remainder of the VSP regime - until VSP legislation is repealed and regulated VSPs are transitioned to the online safety regime.

Our strategic approach to VSP regulation so far

At the outset of the VSP regime, we established our [four broad aims for the VSP regime](#). These are to **raise standards in user protections, rapidly address non-compliance, increase transparency across the industry, and get ready for the online safety regime**. These will remain constant throughout the full duration of the VSP regime.

Last year, [we set out our strategic priorities](#) for the second year of the regime, based on what we had learnt during the first year. We decided to take a broad look at the way platforms set, enforce, and test their approach to user safety, with a particular focus on certain topics, including age assurance. This was the basis for much of the activity outlined in the previous section.

Regulating VSPs remains a priority until the regime is repealed

We are now approaching the final years of the VSP regime. The VSP regime was established as an interim regime. The UK Government will, in due course, repeal the VSP regime and VSPs regulated under the existing regime will transition to being fully regulated under the Online Safety Act 2023 (the OSA).

Until repeal, the VSP regime remains fully in force for all existing services that meet the VSP scope criteria up to the beginning of the transitional period¹⁰ - and we will continue to prioritise enforcing the regime and pushing positive improvements for users for the full duration that it is in place. We'll also work to ensure a smooth transition between regimes, which we discuss further below.

Our strategic approach to VSP regulation going forward

We'll continue working across all our regulatory functions to deliver positive outcomes for users, including policy development, supervision, enforcement, and transparency. To guide our work – and based on what we've learnt since becoming VSP regulator – we're now revising our ambitions for the remainder of the VSP regime.

We drew on several sources to help identify the priority areas we want to tackle for the remainder of the VSP regime. We have:

- taken stock of the insights and learnings we have gained since the start of the VSP regime,
- engaged with civil society organisations on current user safety risks on UK VSPs,
- reviewed information and intelligence from enforcement agencies to gain additional insight into harm prevention systems and processes under the VSP regime, and
- reviewed publicly available intelligence from other regulators, such as the Australian eSafety Commissioner's [transparency reports](#).

We've also ensured that our goals under the VSP regime align with areas that we'll prioritise under the [online safety regime](#) as far as possible. By doing so, our VSP priorities will enable us to deliver a

¹⁰ The transition period began on 10 January 2024, and any services commencing after this date are regulated exclusively under the online safety regime. For more information see Annex 1.

smooth regulatory transition between the regimes and ensure we are prioritising our resources on the areas that impact most on user safety. This approach will also minimise the additional burden on VSPs as they prepare to be regulated under the online safety regime.

Taking all the above into account, we have identified the six priority areas below. We'll continue with our broad focus on how VSPs set, enforce, and test their approach to protecting users. We'll prioritise making sure VSPs have safety measures in place to ensure:

1. **there are clear user policies in place that are easy to find and understand,**
2. **terrorist videos or videos that incite hatred and/or violence are taken down quickly,**
3. **child abusers are prevented from sharing and/or watching child sexual abuse videos,**
4. **children are prevented from finding and viewing pornographic videos on adult platforms,**
5. **children are protected from finding and viewing other age-inappropriate videos, and**
6. **all users can access easy-to-use and effective tools to report content or submit complaints.**

Our overall goal across these priority areas continues to be ensuring that VSPs are taking appropriate measures to protect their users from harmful material.

These are the areas where we will dedicate most of our attention, but we know that other issues might arise that need prioritising due to the severity of harm or risk to users, which we will assess on a case-by-case basis. **We briefly discuss each priority in turn below.**

VSPs have clear user policies in place that are easy to find and understand

It is important for both the VSP and online safety regimes that VSPs have clear user policies in place that are easy to find and understand. This is because user policies make it clear to users what they can and cannot share on the platform, and what platforms will do if a user fails to comply with the platform's user policies.

Our 2023 [report on VSP user policies](#) found weaknesses in platforms' internal and external policies which could result in poor safety outcomes for users. We identified that in many cases users require advanced reading skills to understand platform terms and conditions and terms and conditions were not always comprehensive.

As such, there is more work for platforms to do to make their user policies effective. We will build on the work we have already done and press for further improvements from platforms. Specifically, by the end of the VSP regime, we expect platforms to ensure that their user policies are comprehensive, are easy to find and can be easily understood by users. We also expect platforms to explore and apply approaches to encourage users to engage with user policies.

Having clear and comprehensive terms of service will remain an important requirement under the online safety regime – and remain a core foundation for other measures to improve online safety.

Terrorist videos or videos that incite hatred and/or violence are taken down quickly

Both the VSP and online safety regimes require that platforms protect users from terrorist videos or videos that incite hatred and/or violence, including racist and xenophobic video content. Under the VSP regime, we will continue our work to ensure platforms have in place appropriate systems and processes to identify and remove such video content quickly.

We will continue our work in ensuring that platforms effectively enforce their terms and conditions and look for opportunities to improve takedown times for this video content. Furthermore, where platforms are operating or considering relevant new, potentially risky functionalities – such as live streaming – we want to see platforms giving due consideration to user safety implications and how they can ensure the efficacy of measures to mitigate harms.

Child abusers are prevented from sharing and/or watching child sexual abuse videos

Similarly, it continues to remain a core objective of our work that child abusers are not able to share and/or watch videos containing child sexual abuse material (CSAM). While grooming is not a harm specifically referenced under the VSP regime, grooming activity on a VSP can lead to the uploading or streaming of CSAM. Therefore, we consider it is important for platforms to consider a suite of measures both to prevent grooming and to prevent child abusers from sharing or watching CSAM. Preventing these serious harms will remain a key priority under the online safety regime.

We'll continue to work with our notified VSP platforms to identify and drive improvements in user safety measures that tackle CSAM and grooming. By the end of the regime, we want to be satisfied that VSPs are doing everything they can to identify, prioritise and tackle instances of grooming and the distribution of CSAM, to mitigate the risks of this serious harm.

Children are prevented from finding and viewing pornographic videos on adult platforms

We'll continue our work in ensuring adult VSPs have in place robust age assurance methods which prevent children from accessing adult videos.

We've seen some progress already. Along with the existing verification processes to ensure the age of creators, OnlyFans has introduced solutions, provided by Yoti and Ondato, to verify the age of UK subscribers. This began with new subscribers and OnlyFans have told us they now have retrospectively verified the age of all their UK Creators and were in the process of verifying the ages of all UK fans.

Our [enforcement programme](#) into age assurance measures on UK-established, adult VSPs has also made significant progress on this objective (see above). The programme will continue in the coming year. This engagement will help us to continue to build our evidence base about specific interventions, and how platforms implement them, in turn informing our work under the online safety regime.

This will be highly relevant and important for the online safety regime because sites and apps that display or publish pornographic content must ensure that children are not normally able to encounter pornography on their service. To do this, they must introduce age assurance – through age verification, age estimation or a combination of both – which is 'highly effective' at correctly determining whether a user is a child or not.¹¹ Effective access controls should prevent children from encountering pornographic content on that service.

We will also continue our engagement in this space, including with other VSP regulators in the IWGAV - exchanging information and best practices around approaches to age assurance.

¹¹ <https://www.ofcom.org.uk/news-centre/2023/implementing-the-online-safety-act-protecting-children>

Children are protected from finding and viewing other age-inappropriate videos

We also want to ensure that VSP providers protect children from other forms of restricted material (which includes other material included in videos that might impair a child’s mental, moral, or physical development). We set out examples of the type of content this could include in our [VSP Guidance](#), including video content containing material which is violent and/or content that may promote eating disorders, self-harm and/or suicide, amongst others.

We will continue to work with services under the VSP regime to drive improvements to their child safety measures. For example, we’ll be engaging with VSPs to explore how they can improve methods for identifying children and ensuring they have age-appropriate experiences. As we set out in our [2023 report on child safety](#), we found that platforms popular with under-18s – TikTok, Twitch and Snap - rely on users correctly self-declaring their age on sign up, which is easy to bypass.

Children must continue to be protected from inappropriate and harmful content under the online safety regime. The definition of what sorts of content they must be protected from is slightly different under the online safety regime,¹² but will nevertheless continue to be a top priority for Ofcom. Ahead of the repeal of the VSP regime, platforms have an important opportunity to prepare themselves for their new duties to protect children under the online safety regime.

Users can access easy-to-use and effective tools to report content or submit complaints

Finally, we want to ensure that all users can access easy-to-use and effective tools to report content or complain about platform decisions. We want to shine a light on the measures which most directly enable users to express their concerns to platforms about the content they are seeing, and to seek information from platforms about their decisions.

The ability to flag or report content accurately is a key measure under both the VSP and online safety regimes, and essential to platforms removing harmful content quickly – and, if necessary, enable platforms to prioritise their resources to action content with the greatest risk of harm. By the end of the regime platforms should ensure their content reporting tools are easy to use and access, effective, and cover the full range of harms that VSP providers are required to protect users from.

Where a user wishes to raise a complaint, this should also be simple to use and transparent, and give users sufficient information about the reason for a decision. By increasing transparency about how complaints are handled and focusing on making the process as simple as possible, platforms can empower and build trust with their users, support user understanding of the basis for decisions, and encourage positive behaviours in future. We will undertake some exploratory work on platform approaches to user complaints handling and will push for improvements where needed.

Other areas of wider work

Additionally, we will continue to engage with industry bodies and regulatory counterparts, both nationally and internationally, in pursuit of our aims under the VSP regime, and to promote regulatory collaboration. We also expect our work on VSP advertising¹³, where Ofcom and the

¹² This could include content about suicide, self harm or eating disorders, for example. Further information can be found here: <https://www.ofcom.org.uk/online-safety/information-for-industry/guide-for-services>

¹³ https://www.ofcom.org.uk/_data/assets/pdf_file/0022/229009/vsp-advertising-statement.pdf

Advertising Standards Authority (ASA) work together to regulate non-VSP controlled and VSP-controlled advertising respectively, to continue.

We are committed to continuing to pursue positive change under VSP regime, using the most appropriate range of powers and formal or informal tools to achieve these aims, while remaining proportionate.

More information on repeal of the VSP regime

In May 2023 we published an overview of the [VSP regime repeal process](#). The date of repeal of the VSP regime will be decided by the UK Government.

Schedule 17 of the OSA came into force on 10 January 2024. This sets out the transitional provisions that apply to services regulated under the VSP regime. Now that the transitional period is in effect under the OSA, the VSP regime will not apply to newly established VSPs (being those services that commence provision after the commencement of the transitional period). Such providers are solely regulated under the OSA.

The VSP regime remains live, and we still have powers to regulate existing, UK-established VSPs under the current rules. UK-established VSPs that provided their services prior to the commencement of the transitional period are regulated under both the VSP regime and the OSA although they are exempt from most of the obligations under the OSA until the end of the transitional period. Critically, all VSPs – of which there are currently 22 - are now subject to the new communications offences, Ofcom's information powers and associated enforcement powers, and fee notification requirements under the OSA. VSPs will also become subject to the requirement to complete children's access and risk assessments once a date is specified by the Secretary of State via regulations.

As part of our aim to prepare industry for regulation under the online safety regime, we will work with VSP platforms in their preparations for online safety regulation over the coming months. Our latest roadmap shows how we are planning to implement the regime.

A1 Background

Ofcom has regulated VSPs established in the UK since November 2020

The VSP Regime is set out in Part 4B of the Communications Act 2003 (the Act). In this report, we refer to the regulatory framework set out in Part 4B of the Act as ‘the VSP Framework’ or ‘the VSP Regime’ (referred to as ‘the VSP regime’ hereafter). The requirements for platforms came into effect in November 2020. At the same time, Ofcom was appointed as the regulator for VSPs that have the required connection with the UK.

VSPs must take and implement safety measures to protect users

Under the VSP regime, VSP providers must take and implement¹⁴ such measures as are appropriate to protect all users from videos containing ‘**relevant harmful material**’. Relevant harmful material is video content likely to incite violence or hatred against protected groups, and content which would be considered a criminal offence under laws relating to terrorism; child sexual abuse material; and racism and xenophobia.

VSP providers must also take and implement measures to protect under 18s from videos containing ‘**restricted material**’. Restricted material is videos containing 18-rated or unclassified material, and other material that might impair children’s physical, mental, or moral development. Ofcom refers to relevant harmful material and restricted material collectively as ‘**harmful material**’.

It is for VSP providers to determine the measures that are appropriate and proportionate for their service. However, where providers take one or more Schedule 15A measures to protect users from harmful material, they are required to implement those measures effectively, and in a way that achieves the protection for which those measures are intended.¹⁵

Schedule 15A measures

The measures that VSP providers may choose to take to protect users from videos containing harmful material are set out in Schedule 15A of the Act. These measures include:

- having, and effectively implementing, terms and conditions for harmful material,
- having, and effectively implementing, flagging, reporting, or rating mechanisms,
- applying appropriate access control measures to protect under 18s like age assurance and/or parental control measures,
- establishing easy-to-use complaints processes, and
- providing media literacy tools and information.

In determining which of the measures listed in Schedule 15A are appropriate for their platform, VSPs must have regard to the practicable and proportionate criteria listed under section 368Z1(4) of the Act. These include considering their VSP’s size and nature, the nature of material in question, the harm the material may cause, the characteristics of those who the measure is designed to protect,

¹⁴ [Section 368Z1\(1\) of the Communications Act 2003.](#)

¹⁵ [Section 368Z1 \(2\) of the Act.](#)

and the various legitimate interests at stake, including those of the VSP provider itself, the users who create or upload material, and the general public interest.

VSP providers may also take other measures, not listed in the VSP Framework, which they judge appropriate to meet their duties under the VSP regime and must also take these into account when determining which of the Schedule 15A measures it may be appropriate for them to take. You can read more about the regulatory requirements, the harmful material in scope of the VSP regime, and the measures VSPs must consider taking in the VSP Guidance.

Ofcom's powers

The VSP regime does not focus on whether individual pieces of content are allowed on a platform. Ofcom's role is to ensure platforms have appropriate systems and processes in place to effectively protect their users from videos containing harmful material. We discuss this further below.

Ofcom has powers to take the necessary steps to ensure that VSP providers comply with their obligations under the VSP regime. Our work to secure compliance with the VSP Framework includes ongoing policy development, supervisory engagement with VSP providers, publishing transparency reports, and taking enforcement action as appropriate.

This report is designed to explain how we have worked to ensure that VSPs improve the protection measures on their platforms, using the tools we have available as regulator. The report also sets out our strategic priorities for the remainder of the VSP regime.

Enforcement of the regime

Where we suspect that a VSP has not complied with its duties under the VSP regime, we have a wide range of powers and tools at our disposal. We make an assessment of which tools are most appropriate in any given case in line with our [enforcement guidelines](#), and we'll typically engage with a platform first about our concerns before considering using our more formal tools.

These include opening formal investigations to decide whether a provider is in breach of its obligations, following which we may:

- give the provider an enforcement notification,
- issue financial penalties of up to 5% of the provider's applicable qualifying revenue or £250,000, whichever is the greater,
- require the provider to take steps to come into compliance or remedy the harm caused by the contravention, and/or
- in exceptional cases, suspend or restrict a service.

However, our enforcement activities encompass a wide range of other tools, including:

- sending warning letters outlining compliance concerns,
- opening enforcement programmes to monitor compliance across the sector,
- entering 'compliance remediation' to secure improvements to a provider's measures in lieu of opening a formal investigation, and
- powers to require information to be submitted to Ofcom.

Ofcom has been formally appointed as the UK's online safety regulator

In October 2023, the OSA received Royal Assent, introducing new duties for user-to-user and search services to keep UK users safe online. Ofcom received new powers to regulate online safety and, in

November 2023, published its first Consultation: Protecting people from illegal harms online. Statements following such consultations will set out how services can comply with the OSA over the coming years.

The OSA tackles a much wider range of illegal content and provides a greater set of functions for Ofcom than we have under the VSP regime. Although the two regimes have different requirements, our experience of VSP regulation will help inform our approach to regulating online safety and help prepare us for our broader role. We set out a comparison of the VSP and online safety regimes in more detail at Annex 2.

Ultimately, the UK Government will repeal VSP legislation following a transitional period. From the beginning of the transitional period which commenced on 10 January 2024, VSPs will be regulated under both regimes, but will be exempt from most OS duties under the OSA until the end of the transitional period. Following the end of this transition period all services, including VSPs currently notified under the VSP regime, will be solely regulated under the online safety regime.

A2 Comparison of VSP and online safety regimes

This table sets out in a simplified way the differences and similarities between the VSP and online safety regimes.

	VSP regime	Online safety regime
Scope	Covers only UK-established VSPs. There are currently 22 in-scope platforms.	Include the majority of user-to-user and search services accessible by UK users. Our initial analysis suggests more than 100,000 online services could be subject to the new rules. ¹⁶
Notification	Platforms assess whether they are in scope of the VSP regime and must notify Ofcom if they consider themselves to be in scope of the VSP regime.	No notification to or registration with Ofcom is needed under the OSA. –
Types of Content	The VSP regime only covers shared video content, and does not cover separate ‘surfaces’ like photos, text, search, hashtags or comments. Video is defined as “a set of moving or still images, or of legible text, or of a combination of those things (with or without sounds), which constitutes an individual item irrespective of its length (and which is not an audiovisual commercial communication)”.	Covers most user-generated content, not just video-content and also covers search results. Content defined as “anything communicated by means of the service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.”
Harms	VSP regime covers Harmful Material (includes relevant harmful material and restricted material). Relevant Harmful Material in VSP has limited overlap with Illegal Content in OS (overlaps include terrorism and CSAM). Restricted material includes video-content that is harmful to under-18s including adult material and other material which might impair their physical, mental or moral development.	The OSA’s definition of illegal content is broader than the definition of relevant harmful material under the VSP regime and covers content that amounts to a broader variety of criminal offences (including, for example, offences relating to fraud and the sale of weapons). The OSA also covers content that is harmful to children which includes primary priority content, priority content and non-designated content that is harmful to children. When compared to the definition of Restricted material in VSP, primary priority content that is harmful to children also includes specific references to suicide, self-harm, and eating disorders.

¹⁶ https://www.ofcom.org.uk/_data/assets/pdf_file/0017/270215/10-23-approach-os-implementation.pdf

	VSP regime	Online safety regime
Platform duties	<p>Platforms have a duty to take appropriate measures to protect the general public from relevant harmful material and children from restricted material. Platforms also must implement those measures effectively.</p>	<p>OS duties are broader than duties under the VSP regime and vary depending on the type and category of regulated service in question.</p> <p>Broadly, all regulated user-to-user services are required to conduct risk assessments and mitigate identified risks. They will also be subject to content reporting duties and to duties related to complaint procedures, freedom of expression and privacy.</p> <p>In addition to the above duties, all user-to-user services in scope will have to carry out a children’s access assessment. Services that are likely to be accessed by children will have to carry out the children’s risk assessments and are subject to the child’s safety duties.</p> <p>Regulated search services have similar requirements to user-to-user services, in that they must conduct risk assessments to identify the risks and then take steps to mitigate and manage those risks. They also are subject to the safety duties on content reporting, complaint procedures, freedom of expression, privacy, and record-keeping.</p> <p>Regulated search services also have similar requirements in relation to the requirement to carry out children's risk assessment if such services are likely to be accessed by children and are subject to child safety duties. However, search services differ from U2U services in that their safety duties (noted above) requires the minimising the risk of user encountering harmful material, as opposed to U2U services' safety duties, which require the prevention and at times removal of harmful material.</p> <p>Some platforms are also subject to enhanced duties relating to transparency, user empowerment, and preventing fraudulent advertising.</p>