

Dame Melanie Dawes  
Chief Executive

11 September 2024

Dear Secretary of State,

Thank you for your letter asking about Ofcom's work to protect users from harmful content on 'small but risky' online services. We are keenly aware that while they may not have wide reach, the smallest online services, especially those that host or promote the most harmful content, can represent a significant risk to UK citizens. Tackling these services is therefore a vital part of our mission to make the UK public safer online using our powers under the Online Safety Act.

Although the safety duties are not yet in force, we have already developed plans to take early action against small but risky services to achieve enhanced protections on the areas of greatest harm to users, especially children. The Act gives us a number of tools to set specific rules and to identify, manage and enforce against this kind of service, including through our Codes and by taking enforcement action, using our information powers and using business disruption measures. The particular tools we use in each case will depend on what we judge to be most likely to achieve rapid protection for users. In some cases, for example with services that knowingly or explicitly welcome users whose behaviour is likely to be illegal or harmful, enforcement may be the most effective route. In others, we will seek to achieve compliance through voluntary engagement, where that offers the most rapid way to protect users.

I am pleased to provide more detail here on how we plan to monitor small but risky services, bring them into compliance, and enforce the rules where necessary.

### **Tailoring codes measures to risk**

As you note in your letter, all regulated services in scope of the Act will have to comply with the illegal content safety duties. Any service that is likely to be accessed by children will also have to comply with the protection of children safety duties. In both cases services will need to deploy the measures set out in our Codes of Practice or take alternative effective steps.

In drafting the Codes and Risk Assessment guidance we have proposed that services that pose the most risk should take the greatest precautions. The Codes are explicitly designed so that even where they are small, high risk services will be expected to use greater protections than services that pose less risk. For example, the draft Illegal Harms Codes state that services that pose a high risk of grooming (irrespective of size) should have features which make it harder for perpetrators to contact children. Similarly, the draft Codes state that file-sharing services face a particular risk of misuse by people who wish to share illegal child sexual abuse material (CSAM), and therefore even those with relatively few users should deploy hash matching technology to detect this content. As the codes evolve over time, we will continue to consider where it is appropriate to target further measures at small but risky services.

### **Our proactive approach: Seeking safety improvements from 'small but risky' services via engagement to secure compliance**

In parallel to our approach to the Codes set out in the previous section, we are also developing active plans for supervision and enforcement of the safety duties.

We have established Supervision Teams which are already actively engaging with selected services to drive improvements. The services we have chosen to supervise are those that pose particular risk, **either** because of their size **or** because of the nature of the service. The goal of this targeted oversight is to secure compliance with regulatory duties and improve the safety of UK users, by understanding in detail services' measures, assessing how well they protect users, and pushing for timely improvements where necessary.

'Small but risky' services require a bespoke approach, and we have created a dedicated supervision taskforce for this purpose. This team is developing and delivering a workplan focusing on specific high priority themes (such as CSAM, terror, hate and offences directed against women and girls) in small but risky services. This workplan will target services that present a high risk of harm. Should this type of service choose not to engage and we have evidence of non-compliance, we will move to rapid enforcement action.

We have successfully trialled this approach in our regulation of video-sharing platforms (VSP). A number of small, risky services have improved their policies and content moderation in response to our compliance programme, and others which have declined to make the necessary changes have faced formal enforcement action from Ofcom<sup>1</sup>. Specifically, through this route all of the adult platforms notified under the VSP regime – large and small – have implemented age verification to ensure that under-18s cannot access pornography on their services.

### **Responding to non-compliance from 'small but risky' services: Our enforcement of illegal safety duties and protection of children safety duties**

We already have plans to ensure compliance with the first duties which will go live under Act. These include using targeted enforcement action against small, risky services where there is evidence of significant ongoing risk of harm to users, especially children, and an apparent lack of safety measures in place. We will start to launch enforcement programmes immediately, once the duties have come into force.

Where we consider that a service provider is not meeting its obligations under the Act, we have a range of tools to drive change and improve compliance. We can

- investigate whether a service provider has contravened its obligations, or whether there are industry-wide problems that require a broader response.
- undertake compliance remediation and/or seek commitments to remedy compliance concerns.
- impose penalties of up to 10% of qualifying worldwide revenue or £18 million (whichever is greater), as well as require the service to take remedial action.

We also have statutory powers in relation to certain third parties, including being able to issue them information notices. These measures are set out in more detail in our Enforcement Guidance<sup>2</sup>.

### **Business Disruption Powers**

Furthermore, we have the power to apply to court for business disruption measures in certain cases where enforcement action has not been effective in bringing a service into compliance, including where a service consistently fails to engage with us or take required steps imposed in a decision confirming a breach of the rules. Where ordered by a court, business disruption measures will require third parties such as search engines, payment services, internet access services and app stores to either take steps to disrupt the non-compliant service's business in the UK, such as a search engine removing the provider from search results, or to take steps to restrict access to the non-compliant provider, such as the removal of an app from an app store. In general, given the seriousness of such measures and the high bar to imposing them, we would expect to reserve them for the most serious cases where other measures have not driven the change that is needed. But we recognise that for some services this may be the best or only way of ensuring users are protected.

Finally, the Act gives Ofcom powers to hold tech firms and their executives directly criminally liable for failures to provide us with accurate information, and failures to comply with directions in our enforcement notices in relation to children's safety. While bringing prosecutions under the Act will be reserved for the most serious or deliberate breaches, we are prepared to use the full extent of our enforcement powers where this is appropriate.

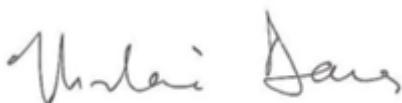
### **Monitoring 'small but risky' services: Our research and triage functions**

You asked how we will monitor small services that pose a high risk of harm to users, including children. To ensure we actively manage the threat posed by small and high-risk services, we conduct ongoing risk research across the industry. This includes data-driven work to identify risk factors across thousands of services, as well as rapid assessments of intelligence from external sources. These tools and processes are helping us identify high-risk services and understand what the best response options might be in each case.

We also have a dedicated Triage team for identifying, prioritising and escalating emerging issues, particularly on services where we do not have an existing supervisory relationship. This team is already in operation and its purpose is to ensure we respond effectively, promptly, and proportionately to new or growing harms and risks, focusing our work on the most credible and high-severity issues where we can have the greatest impact. We examine a variety of intelligence sources to identify new issues, including external reporting, insight from partners, and our own analysis of user complaints<sup>3</sup>.

I hope this further information is helpful in setting out how we intend to combat the risks presented by small but risky online services. I look forward to continuing to work with you and your teams to make a safer life online for everyone in the UK.

Yours sincerely,



**MELANIE DAWES**

---

---

<sup>[1]</sup> Investigations into [My Media World Ltd](#) and [MintStars Ltd](#)

<sup>[2]</sup> See paragraphs A3.11 – A3.16

<https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/annex-11-draft-enforcement-guidance/?v=330409>

<sup>[3]</sup> While Ofcom is not required to respond to and investigate individual complaints, Ofcom has an online form for users to report where they feel a service provider has failed to properly address their concerns. Consumers making a report to Ofcom will have their complaint acknowledged and will be directed to sources of support. Ofcom will analyse these complaints for trends that may require further action. These trends could include a spike in complaints about a new, high-risk service, or uptick in complaints about particularly severe harms on services. When undertaking enforcement activity, Ofcom may consider complaints data to corroborate indications of compliance failure. Where an enforcement decision has been informed by user complaints, Ofcom will usually note that in the decision.