

Your response

Please refer to the sub-questions or prompts in the [annex](#) to our call for evidence.

Question	Your response
<p>Question 1: Please provide a description introducing your organisation, service or interest in Online Safety.</p>	<p><i>Is this response confidential? – N</i></p> <p>Zoom is an American video first, unified communications platform. It was founded in 2011 with a mission to transform video-first unified communications and is headquartered in San Jose, California. Our platform is widely used across the private and public sectors in the UK and elsewhere.</p> <p>The safety and security of our users is a top priority for Zoom, and we have developed a wide range of features to deliver this.</p> <p>We know that, as a service where users are able to communicate over video, audio, and text, that we have an important role to play in ensuring that they are able to do so safely. We engage proactively with politicians, officials, and regulators on issues of online safety, and will continue to do so.</p>
<p>Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?</p> <p>IMPORTANT: Under this question, we are not seeking links to or copies/screenshots of content that is illegal to hold, such as child sexual abuse. Deliberately viewing such images may be a criminal offence and will be reported to the police.</p>	<p><i>Is this response confidential? – N</i></p> <p>Zoom publishes a community standards enforcement report that features the latest data on our Community Standards enforcement actions. The information in the report updates on approximately a monthly basis, in full month increments. The data covers reports that were processed in a particular month, as opposed to reports that we received in a particular month.</p> <p>The report can be assessed here: https://explore.zoom.us/en/trust/community-standards-enforcement/</p> <p>Since Sept 2021, Zoom has processed 140,256 reports for violation of our community standards. 1,544 or around 1% of those cases were from the UK. Actions such as a strike or suspending the user were applied to 68% of our</p>

	<p>UK cases and only 32% of the cases were dismissed.</p>
<p>Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?</p>	<p><i>Is this response confidential?</i> – Y</p>

Question 4: What are your governance, accountability and decision-making structures for user and platform safety?

Is this response confidential? – **Y**

Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?

Is this response confidential? – N

Zoom makes all of our relevant terms of service, policy statements, and guides to best practice for users on using Zoom safely available in a single setting - the Trust Centre. This includes a clearly signposted and accessible link to our Trust Centre resources, including the terms of service and other policy statements.

We believe that this approach, unifying information and ensuring that it is easily accessible, is an important measure that all businesses can take to ensure the clarity and accessibility of the relevant policy statements.

See <https://explore.zoom.us/en/trust/>

Question 6: How do your terms of service or public policy statements treat illegal content? How are these terms of service maintained and how much resource is dedicated to this?

Is this response confidential? – N

Zoom Terms of Service has a general prohibition against illegal content:

“You agree that You will not use, and will not permit any End User to use, the Services to: (vi) use the Services to communicate any message or material that is harassing, libelous, threatening, obscene, indecent, would violate the intellectual property rights of any party or is otherwise unlawful, that would give rise to civil liability, or that constitutes or encourages conduct that could constitute a criminal offense, under any applicable law or regulation;”

<https://explore.zoom.us/en/terms/>

Our Terms of Service are updated on an as needed basis.

Zoom’s Community Standards were written to further explain the specific type of content we prohibit.

<https://explore.zoom.us/en/community-standards/>

The Community Standards are also updated on an as needed basis and we publish a log to keep

track of all updates here:

<https://explore.zoom.us/en/community-standards-update-log/>

Question 7: What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?

Is this response confidential? – N

Zoom makes all of our relevant terms of service, policy statements, and guides to best practice for users on using Zoom safely available in a single setting - the Trust Centre. This includes a clearly signposted and accessible link to our Trust Centre resources, including the terms of service and other policy statements.

We believe that this approach, unifying information and ensuring that it is easily accessible, is an important measure that all businesses can take to ensure the clarity and accessibility of the relevant policy statements.

Zoom also believes that to be effective, reporting mechanisms should be accessible and simple to use. At Zoom, we allow users to easily report abuse in several ways: during a meeting through clicking the top-left "Security" icon, through our web report form, or from the "Meetings" menu in our web portal.

We also regularly post blogs and support articles related to how to employ our various safety features. An example can be found here: <https://explore.zoom.us/en/securing-your-meetings/>

Zoom also has a "Zoom Security Basics" training course in our learning center where users can gain a certificate after completion. The course can be found here: <https://learning.zoom.us/learn/course/external/view/elearning/69/zoom-security-basics>

Question 8: If your service has *reporting or flagging* mechanisms in place for illegal content, or users who post illegal content, how are these processes designed and maintained?

Is this response confidential? – Y

Question 9: If your service has a *complaints* mechanism in place, how are these processes designed and maintained?

Is this response confidential? – N

At Zoom, we allow users to easily report abuse in several ways: during a meeting through clicking the top-left “Security” icon, through our web report form, or from the “Meetings” menu in our web portal.

To ensure we take action on reports about potential violations of our policies in a timely yet diligent manner, Zoom leverages a user reporting system that automatically triages and prioritizes reports of CSAM, terrorism and violent extremism. This triaging process

	<p>ensures we are able to very quickly evaluate, respond, and make reports to the U.S. NCMEC as necessary.</p> <p>We also have a documented escalation and review process, to handle difficult cases. Our four-tiered review system ensures that each report receives proper care and attention.</p>
<p>Question 10: What action does your service take in response to <i>reports</i> or <i>complaints</i>?</p>	<p><i>Is this response confidential?</i> – Y</p>

Question 12: What automated moderation systems do you have in place around illegal content?

Is this response confidential? –Y

Question 13: How do you use human moderators to identify and assess illegal content?

Is this response confidential? – Y

Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?

Is this response confidential? – Y

Question 15: In what instances is illegal content removed from your service?

Is this response confidential? – N

Where content has been flagged and found to be illegal, it will be removed from the Zoom platform.

Question 16: Do you use other tools to reduce the visibility and impact of illegal content?

Is this response confidential? – N

Zoom has also developed a tool to detect if a meeting has a high risk of being disrupted, called the “At Risk Meeting Notifier,” which will automatically alert the account owner by email and provide advice on actions to take where there is a risk of harm.

Question 17: What other sanctions or disincentives do you employ against users who post illegal content?

Is this response confidential? – N

Zoom’s Trust & Safety team is dedicated to dealing with users who share illegal content on

our platform. As the company has grown, so has our Trust & Safety team with the recruitment of experienced and committed team members. The action we will take to cases of illegal content being posted on our platform will range from banning users for relatively minor offences to reporting them to local law enforcement for serious breaches.

Question 18: Are there any functionalities or design features which evidence suggests can effectively prevent harm, and could or should be deployed more widely by industry?

Is this response confidential? – Y

Question 19: To what extent does your service encompass functionalities or features designed to mitigate the risk or impact of harm from illegal content?

Is this response confidential? – Y

Question 20: How do you support the safety and wellbeing of your users as regards illegal content?

Is this response confidential? – N

We have adopted a 'safety by design' approach throughout our product and engineering processes and we are committed to maintaining high standards to prevent and protect against online harms. This includes giving meeting participants the ability to report a disruptive user, and the ability to pause and suspend meetings.

We have also developed a tool to detect if a meeting has a high risk of being disrupted, to prevent instances where a meeting ID or passcode is used by an unintended recipient to cause harm.

Another design feature is our reporting mechanism; meeting participants are able to identify and report other participants in less than four clicks which makes it very accessible for users of all ages.

Question 21: How do you mitigate any risks posed by the design of algorithms that support the function of your service (e.g. search engines, or social and content recommender systems), with reference to illegal content specifically?

Is this response confidential? – Y

Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?	<p><i>Is this response confidential? – N</i></p> <p>We have implemented the ICO’s Age Appropriate Design Code. The code forms a necessary part of the Government’s broader agenda to keep children safe online, improving standards around privacy for online services likely to be accessed by children.</p>
Question 24: Does your service use any age assurance or age verification tools or related technologies to verify or estimate the age of users?	<p><i>Is this response confidential? – Y</i></p>
Question 25: If it is not possible for children to access your service, or a part of it, how do you ensure this?	<p><i>Is this response confidential? – Y</i></p>

--	--

Please complete this form in full and return to OS-CFE@ofcom.org.uk