

## Your response

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

Question	Your response
<p><b>Question 1: Please provide a description introducing your organisation, service or interest in Online Safety.</b></p>	<p><i>Is this response confidential? – N</i></p> <p>The Online Dating Association is the UK registered trade association recognised as the voice of the online dating sector, supported by a membership who believe in trust &amp; safety, honesty &amp; clarity, and privacy; who believe in creating a positive experience for users; and believe in a technology ecosystem that supports innovation in online dating.</p> <p>More here: <a href="https://www.onlinedatingassociation.org.uk/about-us/about-the-oda.html">https://www.onlinedatingassociation.org.uk/about-us/about-the-oda.html</a></p>
<p><b>Question 2: Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?</b></p> <p><b>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.</b></p>	<p><i>Is this response confidential? – N</i></p> <p>The online dating sector is well aware that specific types of ‘priority illegal harms’, as named in the Online Safety Bill, can occur on our platforms.</p> <p>Foremost for us is fraud, and in particular romance fraud. Fraudsters are very clever, and have seen dating sites as easy ecosystems in which to find their victims. However, dating services are aware of this situation, and work very hard to stop fraud from being conducted on their platforms. Utilising machine learning to develop algorithms, content moderation, human moderation and other risk mitigation processes, the prevalence of fraudsters and fraud on dating platforms is much diminished. However, the dating sector is still coping with fraudsters utilising dating platforms to meet potential victims before they are flagged and removed, and then taking the ‘conversation’ with a victim to other platforms (ie Whatsapp). This is why we advise online daters to stay on a dating platform for as long as possible. In fact, recent research shows fraud is now more likely to happen on social media sites than dating sites.</p> <p><a href="https://azbigmedia.com/lifestyle/10-apps-where-people-are-scammed-the-most-in-2021/">(https://azbigmedia.com/lifestyle/10-apps-where-people-are-scammed-the-most-in-2021/)</a></p> <p>Online dating services also grapple with harmful communications, particularly relevant as the three new communications offenses come in with this Bill. Again, the risk mitigation practices of machine learning, algorithms, content moderation and human moderation are constantly used and updated to stop illegal communications harms from happening on dating platforms.</p>

	<p>These are the two major ‘illegal harms’ we see on our platforms, but of course the moderation systems also can stop any other illegal harms (such as CSAM), for which we have no tolerance.</p>
<p><b>Question 3: How do you currently assess the risk of harm to individuals in the UK from illegal content presented by your service?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Online dating services assess the risk of harm to individuals in a number of ways. The Online Dating Association itself has a set of standards, with accompanying guidance, which sets out how services should deal with Trust and Safety.  <a href="https://www.onlinedatingassociation.org.uk/membership/standards-guidance.html">https://www.onlinedatingassociation.org.uk/membership/standards-guidance.html</a></p> <p>Every member of the ODA is actively working on mitigating harm. While bigger dating services have processes to follow when a new product is developed or a new harm identified, smaller organisations have a less formal process. For instance, for one ODA member, when a new product feature is developed, the product designers, compliance officers, head of customer service, and moderators all sit down together to brainstorm how the new product could be used negatively – pooling their expertise of dealing with users. This means many potential negative uses of a feature can be planned for, and therefore the risk mitigated.</p> <p>Another, very small member, shared with me that because they are personally involved with their dating website, they are always thinking in a ‘risk management’ mindset, and can deal with the constant evolving nature of new risks to online daters on their platforms.</p> <p>Some Associate members of the ODA (ie services that support the online dating sector) are actively involved in risk mitigation before it reaches the platform level, wherein they go into the dark web to see what fraudsters are planning, sharing and preparing. Many dating services utilise these options to better risk assess and protect their services.</p>
<p><b>Question 4: What are your governance, accountability and decision-making structures for user and platform safety?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Governance and decision-making structures at big companies with multiple services are handled by specific teams with experience utilising clear structures and frameworks. For instance, Legal and Trust &amp; Safety teams will attend Product design meetings and weigh in if a new development increases risk, based on their experiences. There is also often a dedicated safety engineering team responsible for building appropriate infrastructure to operate safety</p> <p>For smaller companies, it’s embedded in the culture and feedback loop between the Product team, the Risk team and the Customer</p>

	<p>Services team for combating emotional and financial harms. For many of our smaller members, the lead for both Product and Customer Services may be the same person, and this person will liaise with the Director/CEO regularly to highlight customer experiences and complaints. A Risk team may focus on tackling the financial harms from scammers and have internal tools and development resources to enhance the detection of bad actors</p> <p>So there is often not a ‘paper trail’ for risk assessment for user and platform safety, but a constant ‘safety by design’ mindset which means teams are constantly working to improve the experience of their users and protect them from harm.</p>
<p><b>Question 5: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>The ODA makes clear how important Terms and Conditions are for user experience on dating sites. We also advocate for the use of a code of conduct for users.</p> <p>On our website you can find a section of our standards on ‘honest and clear communications’.  <a href="https://www.onlinedatingassociation.org.uk/membership/standards-guidance/honest-clear-communications.html">https://www.onlinedatingassociation.org.uk/membership/standards-guidance/honest-clear-communications.html</a>) This highlights how important Ts and Cs are, <b>including the problematic practice of misleading by omission.</b></p> <p>Some services provide regular reminders of Terms and Conditions and the code of conduct, particularly if a user is flagged for inappropriate behaviour. The Ts and Cs also give the service legal grounding for removing a user.</p>
<p><b>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?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Most dating services make notice in their terms and conditions of what actions are and aren’t allowed on their services. This always includes forbidding illegal content on the services. Many dating services also make public statements about illegal content – for instance, dating services have been vocal about their work to stop ‘cyberflashing’ or their support for combatting violence against women and girls. The Online Dating Association standards also are clear terms and conditions should include how the service will deal with illegal content.</p> <p>The terms of service form the core of the community for online daters. These are what are referred to when a user is either flagged, sandboxed, or removed.</p> <p>A huge amount of resource is dedicated by dating services to the removal illegal content. As our chat functions are not encrypted, they</p>

	<p>are scanned for illegal content (and harmful content) by machine learning, and then flagged profiles/message are sent for human moderation. There are a number of third-party services who are working to solve many of the challenges for online dating – from background checks, content moderation and personal safety to dealing with financial fraud. We take keeping our users safe very seriously.</p>
<p><b>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?</b></p>	<p><i>Is this response confidential?</i> – N</p> <p>Online dating services, especially ODA members, are very clear in their terms and conditions. As mentioned above, the ODA sets a standard for the quality of Ts&amp;Cs. Many also have community guidelines.</p> <p>These set the scene for positive interactions between users, but also for the awareness of users to report complaints. By having clear Ts and Cs and guidelines, user know when they have experienced something harmful or unwanted and are able to report it through simple push button actions.</p> <p>Most dating services also make clear what will get users banned, so the knowledge is clear ahead of time. We are always working with our members to improve the communications between the company and the user.</p>
<p><b>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?</b></p>	<p><i>Is this response confidential?</i> – N</p> <p>All ODA members, and most online dating sites and services have a reporting and flagging mechanism.</p> <p>These are usually built over time through data collection and utilising machine learning to build algorithms to continually improve the flagging process. Flagged messages or profiles can be moved to human moderators, who are then able to move the message into a 'sandbox' (where in the user cannot tell the message hasn't been delivered) or move the whole profile to a sandbox for further investigation (where the user cannot tell they have been temporarily removed), before removing it already. Third-party content moderation providers, which are proliferating, are able to offer this as a service externally to online dating platforms and many start-ups and SMEs in the sector are utilising this option.</p> <p>The communities on many dating services are also engaged with keeping fraudsters, harassment and underage users off the platform so make use of reporting mechanisms. This is hugely beneficial to moderation teams, who are able to then review profiles or messages flagged from within the community. ODA recommends all dating services have a well-functioning reporting system.</p>

	<p>These processes are either designed in house and developed and improved over time; or they are contracted out to a third party supplier who has built highly impactful algorithms from multiple platforms and can tailor a moderation service to each platform, utilising both flagging and reporting.</p>
<p><b>Question 9: If your service has a <i>complaints</i> mechanism in place, how are these processes designed and maintained?</b></p>	<p><i>Is this response confidential?</i> – N</p> <p>Complaints mechanisms, for most dating services, have been developed over time. All ODA members have a complaints mechanism, and the design of these depends on if the service is an app or a website. In our standards, we strongly recommend a complaints process.</p> <p>These are staffed by complaints and customer service teams (for the big members) or by the core small team, for our smaller members.</p>
<p><b>Question 10: What action does your service take in response to reports or complaints?</b></p>	<p><i>Is this response confidential?</i> – N</p> <p>Our standards suggest ODA members should deal with all complaints. ODA itself used to run a complaints service, until this became too difficult to manage.</p> <p>Large dating services and companies with multiple brands have a multilayer complaints service/teams. Small and medium size dating services often deal with complaints directly.</p> <p>Reports are dealt with by the moderation teams, which sometimes fall under the customer service heading, and sometimes are an entirely separate team. Reports usually mean a profile is flagged, and then it is moved to the human moderation teams who investigate the profile or message further. If the content is contrary to the Ts and Cs, the user will likely be banned.</p> <p>Sometimes, companies will utilise a ‘sandbox’ to move a profile into which has been reported and/or flagged where the profile can only talk to other scammers (for instance). This allows the machine learning to increase its education in how scammers act and engaged, and it keeps the scammer busy talking to other scammers. This practice helps improve the overall content moderation.</p> <p>Complaints are very important to dating services as users having a positive experience is essential to their success. As a product which is ‘designed to be deleted’ reputation and word of mouth recommendations are necessary. However, there are some ongoing concerns with some online dating services that complaints are not dealt with appropriately. Dating is a highly personal experience, and it is essential complaints processes should take into account mixed messages, differing opinions and context.</p>

<p><b>Question 11: Could improvements be made to content moderation to deliver greater protection for users, without unduly restricting user activity? If so, what?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>There is always a balance between content moderation and user experience. The more hurdles that a customer must overcome during the KYC and profile set up stage, the more likely the user is to not enrol on the platform.</p> <p>In the dating sector, content moderation is done in a number of ways. It may be done in-house using machine learning to develop algorithms over years of use, which will do the automatic scanning and flagging, which is backed up by a team of moderators.</p> <p>Many dating services also use third party providers of moderation services. These providers have developed high quality content moderation across different sectors in text, voice and video and are able to apply these to the specific dating service, and utilise ‘rules’ for the service which match the Ts and Cs.</p> <p>Improvements are constant for dating services and content moderation. Each new product design must have content moderation practices to match.</p>
<p><b>Question 12: What automated moderation systems do you have in place around illegal content?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Most dating services have some level of automated moderation system in relation to text, voice and video. The automated systems read messages and check profiles, flagging concerning content for human moderation.</p> <p>Any dating service that does not have an automated system does all moderation by human, as they are small and bespoke.</p>
<p><b>Question 13: How do you use human moderators to identify and assess illegal content?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>For small dating services, as stated, the moderation may be all done via humans – so each profile would be checked by a person and any flagged or reported message by humans. Many of the small services have tight knit communities and users are quick to report bad behaviour or concerns and have direct interaction with the moderators.</p> <p>For bigger services, human moderation comes after the automated systems. Flagged content or profiles will be passed from the automated system to a human moderator for decision.</p>

<p><b>Question 14: How are sanctions or restrictions around access (including to both the service and to particular content) applied by providers of online services?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Please see previous answers around why a user will be sandboxed or banned from an online dating service.</p>
<p><b>Question 15: In what instances is illegal content removed from your service?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>All illegal content that is found by automated moderation, human moderation or reported by users is removed. The account that posted the content is usually first ‘shadowbanned’ or ‘sandboxed’ while human moderators examine the profile. If the profile was found to have posted illegal content (or any content against the Ts and Cs) it will be removed.</p>
<p><b>Question 16: Do you use other tools to reduce the visibility and impact of illegal content?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Messages that contain questionable content are often stopped from delivering, even before a profile is removed. If words like ‘send money’, or swearing, or inappropriate content are detected, the messages may be ‘sent’ but they are never delivered and held for moderation. This can also be done with photographs, such as unwanted cyberflashing. This helps the received have fewer poor experiences online.</p>
<p><b>Question 17: What other sanctions or disincentives do you employ against users who post illegal content?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>In dating, the removal of profiles and banning from the app or website is quite a good disincentive. We do regularly deal with banned profiles trying to create new profiles, and this is where we use technology related to IP addresses, text and language used, geographical location etc to remove users to try and return to a platform after being banned.</p>

<p><b>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?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>All the moderation practices we use can and are deployed across different verticals in the tech world. It is useful that the third-party services are utilise in many tech sectors as it improves their overall moderation systems.</p> <p>There are also opportunities such as ID verification that can stop some harm, however we are still to see how well these safety tech services work with dating, and would not advocate for this to beon mandatory at all.</p>
<p><b>Question 19: To what extent does your service encompass functionalities or features designed to mitigate the risk or impact of harm from illegal content?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>As expressed above, every part of a dating service is designed to stop harm to its users. From safety education centres to automated content moderation, liveness checks, and human customer service, dating services want all users to have a positive experience online dating and these means making sure users do not experience harm.</p>
<p><b>Question 20: How do you support the safety and wellbeing of your users as regards illegal content?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>As above, dating services work hard to keep illegal content of their platforms.</p> <p>If something illegal is reported and flagged, dating services may reach out to the individual and if a crime has been committed, such as romance fraud, the individual may be encouraged to report the crime to the police.</p> <p>The safety centres of many dating services also have helpful guidance and mental health support.</p>
<p><b>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?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Dating service algorithms are focused on ‘matching’. So, the algorithms are learning what each user likes (geographic location, activities etc) and will then refine the matches for each user. This isn’t particularly related to illegal content, because illegal content is flagged and remove and not part of the algorithms.</p> <p>However, as described above, algorithms do come into play with content moderation systems. They learn, through experience and rules, what is and is not flaggable. However, ODA members would not remove a profile based solely on automatic content moderation but</p>



	<p>would move the content/profile to human moderation which deals with the risks posed.</p>
<p><b>Question 22: What age assurance and age verification technologies are available to platforms, and what is the impact and cost of using them?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Dating services are designed for those over 18.</p> <p>Many dating services utilise difference age assurance methods. All will ask for a birthdate, and if this is under 18, remove the profile and note the IP address associated.</p> <p>Many have developed high quality machine learning methods that can spot underage users who have successfully lied about their age. This can be through scanning of images, text or audio, with lots of flags indicating a user might be underage. This will then ‘sandbox’ the profile until the user can prove they are over 18. If they cannot, the profile is deleted.</p> <p>Finally, there are ‘age-verification’ methods, which range from connecting to social media accounts, to liveness and ‘age-estimation’ checks, to showing Government ID, to checking a user’s existence against existing records. None of these have proven perfect in delivering age-verification, so a service stating they use one ‘age-verification’ provider does not mean children are not on the service. In relation to apps, we would suggest Google and Apple should be more involved with age-assurance, as if an app is downloaded through the app stores, Google and Apple will know the age of the user.</p> <p>However, age-verification is not clearly defined and there are many providers of very differing qualities that provide age-verification. Therefore, if Ofcom is considering requiring any age-verification process, it must take into account the quality, potential negative impact on users, and how quickly technology may move on from what is available now. We still strongly advocate for an outcomes-based framework here, with the outcome being those under 18 are not on the platform.</p>
<p><b>Question 23: Can you identify factors which might indicate that a service is likely to attract child users?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>Well known services may attract the interest of teenage users, but dating apps are not designed nor advertised to children, therefore if there are attempts to access them by children, this is the child going against the Ts and Cs of the platform. They will be removed.</p>

<p><b>Question 24: Does your service use any age assurance or age verification tools or related technologies to verify or estimate the age of users?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>As described in Question 22, dating services use many different age assurance methods from entering a birthdate, to machine learning tactics to observe actions by likely children, to showing Government ID, to using new safety tech age-verification methods such as age estimation.</p>
<p><b>Question 25: If it is not possible for children to access your service, or a part of it, how do you ensure this?</b></p>	<p><i>Is this response confidential? – N</i></p> <p>As above, by doing the utmost to stop children accessing the service. What the sector, and all tech needs, is flexibility in constantly looking for the next technology that can be closer to ‘perfect’. We would advocate that no one type of age-verification or age-assurance is mandated.</p>
<p><b>Question 26: What information do you have about the age of your users?</b></p>	<p><i>Is this response confidential? –N</i></p> <p>Our users are all over 18. If they are found not to be, they are removed. The ODA also recommend their data is removed.</p>
<p><b>Question 27: For purposes of transparency, what type of information is useful/not useful? Why?</b></p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>
<p><b>Question 28: Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?</b></p>	<p><i>Is this response confidential? – Y / N (delete as appropriate)</i></p>