Consultation response form

Your response

Question	Your response
Question 1: Do you have any comments on Ofcom's proposed Plan of Work 2023/24?	**Who we are** Match Group operates a portfolio of online dating services across the globe for individuals age 18+. Well-known brands in the portfolio include Tinder, Hinge, Match, PlentyOfFish, OkCupid, OurTime, Meetic, and Pairs and each is designed to increase our users' likelihood of finding a romantic connection. Through our portfolio of trusted brands, we provide tailored products to meet the varying preferences of our users. We currently offer our dating products in 42 languages across more than 190 countries (Group official website: http://mtch.com), including in the United Kingdom. We are grateful for the opportunity to respond to this consultation and share our views regarding Ofcom's existing workplan and future priorities for 2023/24. As part of our commitment to online safety, Match Group values the opportunity to work in partnership with Ofcom and other regulatory authorities, such as the Competition and Markets Authority and the Information Commissioner. We very much believe that when industry and regulators such as Ofcom work together towards common goals that the safety of all UK online users is appropriately enhanced. Match Group is committed to working productively and cooperatively with Ofcom and to sharing our views on the best approach to the unique safety needs of our users. In fact, we recently responded to your call for views on the first stage of your online regulation in September 2022, and we will be responding to the second consultation in due course.

Our proposal for a holistic approach to the UK's online safety regime

As noted in the proposed plan of work, driving the implementation of robust age assurance to protect children from adult content will be a crucial element of protecting the most vulnerable users (children) from online harms such as gambling, pornography and other age-inappropriate content. Match Group is fully supportive of these aims. By choice, Match Group limits the use of our services to those who are 18 years of age and older. We have made this choice because we strongly believe it is the right thing to do. Additionally, we recognize our role in the app ecosystem to lead by example and we are proud of our past and ongoing efforts to make the online experience a safer one for all users, not just our own. We know we are not alone in this view, and we hope that other service providers will more publicly support the work of Ofcom and other agencies.

To meaningfully improve safety for the whole of the online community, we encourage regulatory bodies to examine the issues holistically, importantly ensuring that both app developers and the companies that distribute apps (app stores) do more collectively to ensure that children are appropriately kept away from adult applications and content.

Match Group works tirelessly to keep individuals under the age of 18 off our platforms. However, despite all our efforts to detect and remove underage users, to be more effective a community effort is required. This means that every company that interacts directly with consumers must step up and do its part, including the distribution layer of the digital economy. Meaning the application stores (also known as "app stores"). Due to seismic changes in the mobile phone operating system marketplace brought upon by the lack of competition, Apple on iOS and Google on the Android operating system, now have

monopoly control of app distribution marketplace. Apple and Google play an important role in the app ecosystem, yet despite this fact, they have generally refused to work cooperatively with Match Group brands on key safety initiatives. For example, as noted above, Match Group by choice has decided to limit the use of our services exclusively for individuals who are 18 years of age and above. Despite this and our numerous appeals to Apple, it still lists our brands as being appropriate for individuals "17+". Further, both Apple and Google refuse to share user information they are in possession of that would inform Match Group and other responsible developers seeking to fence off young users.

To fix this problem, online services (including those offered by Match Group portfolio brands) would benefit from regulation strategically designed to enhance online safety in the digital economy as a whole. App stores are not currently recognized as a service category within the Online Safety Bill, despite being the gateway to the majority of digital content for both adults and children. As envisioned currently in the legislation, it appears that the app stores were incorrectly thought to play no role in promoting or enhancing online safety. Match Group can attest to the fact that the stores must play a key role if we are to protect our children. We strongly encourage all appropriate UK officials to not settle for half measures when it comes to protecting our children and instead fight for real solutions.,

To be clear, we are not advocating for any diminution of responsibility away from developers and providers of user-to-user services. For Match Group, working to create a safer online experience for our users is not just the right thing to do, but it is also a good business decision. However, in our view, user safety must not be segmented to certain user experiences and not others. With this in mind, we hope the UK will continue to be one of the

most forward-looking countries when it comes to safeguarding our children.

In our view, it is crucial that Ofcom examine this issue in the workplan for 2023/2024, considering the role which app stores themselves play in the digital economy, and examine app stores' potential obligations under the new online safety regime as well as the existing efforts of Apple and Google to contribute to a safer internet. We would ask that Ofcom investigate this proposal and its implications for a better, more holistic online safety regime, and we reaffirm our offer of support to Ofcom for any insight that Match Group can provide.

Match Group wants to highlight the following safety initiatives elaborated below.

Age gating on our platforms

- With the combination of technology and human moderators, Match Group works diligently to keep underage users off our platforms. In addition to using sophisticated artificial intelligence, our brands collect birthdates, phone numbers, pictures, bios and other inputs when/where available that we use for age verification. We also scan profiles for red flags to keep underage users off our platforms. Human moderators also review accounts that have been flagged either by automated systems or by user reports, and act on those reports accordingly.

Moderation at account creation

- Accounts are reviewed as the profiles are created.

- Both images and text are reviewed for underage signals.

Ongoing moderation process to check and scrutinise profiles

- Accounts are subject to regular detection and scrutiny mechanisms.
- The moderation process led by our Trust & Safety team is enhanced by the vigilance of our members who are encouraged to report any suspicious profiles.

We work closely with legislators and regulators across the globe to contribute to the agreement of new safety-focused standards and laws, to help make both our own and other internet users safe. We appreciate the responsibility we have as a major service provider to shape the regulatory environment for the benefit of all online users, not just our own members.

We continually review our safety protocols in line with best practice to ensure that online safety, including protecting consumers from online fraud and scams, remains a top priority. We are also acting proactively in advance of the introduction of the Online Safety Bill, a landmark effort to improve online safety which we fully support.

Our work in advance of the Online Safety Bill

Match Group brands invest meaningful resources, both in terms of capital and human resources, with the aim of providing a safe user experience. The focus on safety begins at registration and continues throughout our members' user journey on our platforms.

These measures have been introduced in advance of global legislative efforts to make the online world a safer place for users. We are fully in support of efforts that have been made by legislatures on all continents, from California to Australia, which will make a difference in creating a safer experience for all

users. Above all, we believe that the safety of underage users must be the priority for legislators, and we are grateful that both the UK Government and Ofcom have acknowledged that the wellbeing of children and young people must come first.

Match Group agrees with Ofcom's assessment in the proposed workplan that a priority outcome must be to help UK citizens to live a safer life online and that member safety should be embedded at the heart of online services' decision making. Our platforms are being proactive to ensure that they are fully compliant with the Online Safety Bill's provisions, and we are going further to demonstrate best practices to the online dating industry.

We are already introducing safety features using both human moderated and automated tools to identify, remove and block potentially harmful content and inform our members of how they can protect themselves when interacting on our platforms. We were proud to recently [announce new safety features](#) on Tinder and Meetic which will prompt members with in-app messages to advise them about problematic or dangerous behaviours and offer tips for members to interact more safely online. These scam-related tips will be available to members from today in more than 15 countries, including the UK.

Our tips will start to be displayed to members around the world throughout the month of January via an in-app message in the Tinder and Meetic's apps, and notifications to members on Match, Hinge, Plenty of Fish, and OurTime. This global public awareness campaign will help to educate daters and consumers on how to date safer and help stay protected against different forms of online fraud.

Often, fraud occurs when the scammer attempts to move a member from our platforms – a safer, monitored environment – to another

separate platform where we can't moderate or warn members of potential scams. We recently launched a feature which sends our members a popup message with safety tips about romance fraud, crypto scams and other safety tips if our artificial intelligence detects certain words and phrases associated with scam behaviour.

Match Group, along with law enforcement and cyber-crime investigators, developed these tips to help members identify and help prevent and report malicious actors - on dating or any online platform.

As well as these recent measures being introduced to combat romance fraud, we have been the first to introduce innovative measures such as our partnerships with non-profit and non-governmental organisations to develop our approach to trust and safety, including reporting and content moderation, as well as specific concerns like loneliness, anti-sexual violence strategies and child safety.

All our brands have the ability for members to make a report in-app or contact our Trust & Safety teams. If a member contacts us to report a concern, our teams review the report and take the necessary action to remove any profile which violates our Terms of Service from our platform. For the most serious offences, we will proactively ban member accounts across the Match Group portfolio.

- This reporting has been further enhanced with new features like 'Are you sure?' on **Tinder**. Using artificial intelligence (AI), the app identifies and flags potentially harmful or offensive messages while they are still being drafted, asking the member "Are you sure […you'd like to send this message…]?" before they send it. The feature is the mirror image of a safety feature previously introduced in the app, "Does this

bother you?", where if a member receives a message that Tinder's AI deems inappropriate or potentially abusive, the recipient will be asked in a pop-up message: "Does this bother you?". If the answer is yes, they can report the sender.

- On **Meetic**, we seek to shape member behaviour, helping them to feel safe and empowered by encouraging reporting. We identify patterns of member behaviour that might suggest misconduct - for example, when a member sends out a certain number of messages without any response from the recipient, it can indicate potential harassment. When this threshold is reached, an advice message is shown to both the sender and recipient of the messages. This is intended to encourage the recipient to report harassment so that the Trust & Safety team can review and take enforcement action where appropriate.

Our focus is on facilitating positive and safe real-life member experiences, and we see a high risk in allowing potentially bad actors to continue using our service. Members may report concerns from multiple places inside the app (i.e., each profile, messages view, and through general reporting), and non-users have the ability to make reports through either an email to our customer care team or through a reporting flow in our FAQs. We spend considerable effort and resources to process and act on reports.