Written evidence submitted by Match Group (OSB0053)

Executive Summary

1. Online dating has played a pivotal role in shaping todays' internet savvy society and the way personal relationships are formed. One in three marriages begins on an app and in the US, 40% of all relationships and 65% of all LGBTQ+ couples meet online.

2. As a market leader in online dating services, Match Group strongly supports and believes it is right for government to scrutinise market players across the digital ecosystem. Match Group welcomes the opportunity to engage with the UK Government on online safety and consumer protection, hoping to see the level playing field and standards that Match Group adheres to applied across the sector by all market participants.

3. This document includes an overview of Match Group, its brands and the format of our business model. Responses to questions in the call for evidence have also been provided.

About Match Group

4. Match Group is a leading provider of online dating services across the globe. We operate a portfolio of trusted brands, including Tinder, Match, PlentyOfFish, OkCupid, OurTime, Meetic, and Pairs, each 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, including in the United Kingdom where some of our main brands are widely used.

6. Our platforms are mainly closed networks enabling private, peer-to-peer communications between adults, enabling them to establish a meaningful connection in real life. Our platforms are not social media enabling one-to-many communication nor do they rely on selling targeted advertising to make money, as 98% of our revenues come from subscriptions paid by users.

7. As a result, our business model generally focuses on facilitating in-person interactions as a result of 1-1 messaging. The aim of our business model is therefore to reduce online dependency, meaning we want users to move away from online connections to offline in-person relationships. In contrast, other businesses are trying to move more of people's time online to support revenue streams like the sale of advertisements and the harvesting of personal data.

8. We understand the social responsibility that comes with online dating, and Match Group takes the online safety of its member community and potential users seriously; any misconduct on our platforms is one incident too many. The policies that Match Group currently have in place provide a solid foundation on which to tackle online harms within Match Group and across the digital ecosystem.

9. Our market leading position and the responsibilities that come with this are not lost on Match Group. We continually review our safety protocols in line with best practice and ensure that online safety, including protecting consumers from online fraud and scams, is equally prioritised as much as the user experience.

10. All Match Group platforms have built-in tools which are specifically designed to promote the responsible use of our platforms and tackle any potential illegal, illicit, or harmful behaviour. The policies that Match Group currently have in place to protect users online and increase online safety provide a solid foundation on which to tackle online harms within Match Group. We believe these could be replicated across other areas of activity in the digital ecosystem.

11. Match Group brands invest meaningful resources, both in terms of capital and human resources, with the aim of providing a safe user experience. Our customer care team represents 20% of our workforce. The focus on safety begins at registration and continues throughout our members' user journey on our platforms. We have spent hundreds of millions on product, technology and moderation efforts related to trust and safety in 2021 to prevent, monitor and remove inappropriate, illegal, or harmful content.

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

12. Our market leading position and the responsibilities that come with this led to the development of various internal mechanisms to safeguard consumer safety on our platforms.

13. The draft Online Safety Bill goes a long way to consider safety and the risk of harm online more generally. However, more focus could be placed on the ways in which tech companies use their platform design and systems and processes to protect their users. Currently it states that "they have a duty to operate such systems and processes" but does not explicitly state what these would look like on the various platforms.

14. We welcome additional guidance in the form of Codes of Practice for companies to adopt greater consideration of safety within platform design. However, we believe that overly prescriptive processes, if published in the public domain, could potentially undermine safety efforts by providing bad actors with intelligence to circumvent protocols. As it stands, the draft Online Safety Bill is well positioned to maintain safety protocols without eroding necessary privacy standards to reporting users.

Will the proposed legislation help to deliver the policy aim of using digital technologies and services to support the UK's economic growth? Will it support a more inclusive, competitive and innovative future digital economy?

15. Match Group believes that a successful digital economy is based on inclusivity, a fair and competitive market and the safeguarding of users' rights. We recognise the importance of interacting securely across borders and ensuring businesses can compete globally, which ties into the Government's Global Britain agenda and wider ambitions.

16. Match Group notes the joint DCMS and BEIS consultation on a new pro-competition regime on digital markets and will respond separately to both. Competition is key to unlocking the full potential of a digital economy; however, the unprecedented concentration of power amongst a small number of digital firms is holding back innovation and growth. This legislation is only one element towards the contribution of an innovative future digital economy and, without suitable measures to complement it, can only do so much.

17. Nonetheless, this legislation will also portray the UK as a leader in online safety. The UK will be the first country to comprehensively regulate social media platforms in this way, and we are confident other countries will seek to emulate this model.

Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?

18. The measures proposed in the draft Bill provides a good framework for protecting underage users and children from harm they may encounter online.

19. However, having an explicit definition and process for determining harm would not reflect variation across platforms, brands, and industries, and the constantly changing nature of harms. Different industries are likely to see different issues, and different harms may result from the same behaviour. For example, a 16-year-old interacting with a 40-year-old in the comments section of a news source is very different from a 40-year-old trying to talk to a 16-year-old on social media or a dating app.

20. Our moderation efforts are as rigorous for a 16-year-old as they are for a 40-year-old. We moderate everyone 18+ the same way, but we are also looking for underage users to ensure our platforms are moderated in as much detail as possible. By preventing underage access to our platforms, we can prevent instances of grooming and related harm to children. As with most of our platforms, we do not let users exchange content on our platforms, such as pictures and videos, like you are able to on social media. The main risk to children, therefore, is not content but interactions, where grooming could take place.

21. The policies that Match Group currently have in place provide a solid foundation on which to tackle online harms within Match Group and across the digital ecosystem. To keep underage users off our platforms, we:
    - Ask registering users to input their date of birth to indicate their age (this is more effective than saying "for adults" as it catches users that provide an underage date of birth and blocks them until they turn 18);
    - Explicitly ask registering users to confirm they are old enough to use our services when agreeing with our T&Cs;
    - Scan all profile pictures using automated tools to determine the age and all flagged pictures are double-checked by a human moderator (we deliberately use on a high rate of false positives); and
    - Actively monitor our platforms to detect suspicious profiles and take swift action to remove them. We also rely on other users to report suspicious profiles.

22. At the moment, however, there are instances of underage users finding their way onto adult platforms. A recent Guardian[1] article found that an investigation uncovered instances where Apple allowed underage users access apps intended for adults, despite having asked for and recorded their dates of birth.

23. Age verification is important to Match Group and we support efforts to improve age verification through reasonable regulation. To do this, we would propose a solution similar to what has been done in other industries. In general, where obligations to verify age exist prior to the purchase of a good or service, it is imposed at the "distribution layer" of the

[1] https://www.theguardian.com/technology/2021/aug/25/apple-allows-children-to-access-casual-sex-and-bdsm-apps-finds-report

consumer retail chain. For example, when a Heineken-brand beer is purchased by a consumer, Heineken does not verify the age of the consumer. Instead, that obligation rests with the retailer which is distributing the product to the consumer – whether a bar, restaurant or supermarket.

24. In the world of mobile devices and computers, the same model should be applied. The tech platforms that control the access points, or "distribution layer", of the internet — largely tech giants who develop operating systems, app stores and browsers — already have age information or could easily obtain it. Like bouncers standing at the door of the internet's distribution layer, these tech giants already only permit entry after extracting all sorts of information through an account setup process or cookies, such as name, address, age, credit card and phone numbers, location and usage data, etc. They then use this information to power their commercial interests — for example, ad tech platforms (i.e., Google Ad Network) and payment processing systems (i.e., Apple Pay) — all while ignoring the primary responsibility of a bouncer: ensuring underage users do not access content not intended for them.

25. Similarly, we prioritise the safety and wellbeing of our legitimate users, and that means believing user reports and taking swift action to protect our communities. At the same time, users whose online content on their public profile has been removed, or whose profile has been banned following a complaint stemming from 1-1 conversation on a platform, can request a review of that decision to our customer service teams.

26. We are very willing to engage with users who seek a review of the decision not to accept them on our platform because they were deemed underage – in this instance, we act in order to protect their own safety outright and we tell them so. However, we believe that an appeals process allowing a user who has been reported as potentially posing a safety risk to others needs to be very carefully designed.

27. Indeed, an appeals requirement transposed to online dating without consideration of a process where people are supposed to interact first online, and then meet a in real life, could put our users at risk. For example, telling an abuser that they were reported by the abused party for such abuse, especially when the abuser may be able to interact with the abused party in real life, could result in an event greater risk to the reporting user. This could be exacerbated further if the abuser had already met with the abused party.

<u>Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?</u>

28. Match Group believe that the appeal process and feedback mechanisms need adapting in order to avoid further harm. We believe that providing detailed reasons to a user about why their content has been taken down could be problematic in some cases. For example, telling an abuser that they were reported by the abused party for such abuse could put the abused at further risk if the abuser knows personal information about them.

29. As such, the draft Bill must accommodate the range of interactions across the digital ecosystems, their differences and the physical and mental risks posed through overly detailed review / appeals mechanisms.

Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g., safety by design, algorithmic recommendations, minimum standards, default settings?

30. Match Group brands invest meaningful resources, in terms of both capital and human resources, with the aim of providing a safe customer experience and have developed multi-layered systems against illegal content. Safety is and has been built into our applications, and we are continuing to formalise our safety by design protocols.

31. Our market leading position and the responsibilities that come with this led to the development of those various internal mechanisms to safeguard consumer safety at our platforms.

32. We welcome additional guidance in the form of Codes of Practice for companies to adopt greater consideration of safety within platform design.

Does the proposed legislation represent a threat to freedom of expression, or are the protections for freedom of expression provided in the draft Bill sufficient?

33. We support providing explanation about the removal of harmful comments on social media. However, it is a problem for online dating platforms as our aim is to get people off our platforms and meeting in person. If we were to tell an abuser that we have banned them from our platform and they had already met with the abused party, this puts the latter at a greater risk. Furthermore, bad actors may take advantage of the knowledge of the rationale for their ban to circumvent safety policies. We do not believe that the necessary protections we have in place for our users pose a threat to freedom of expression in this context.

The draft Bill specifically *includes* CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

34. We would agree that these two types of content are priority areas. From a moderation perspective, identifying CSEA is relatively straightforward to spot, as is terrorist content. Beyond this, however, illegal content is often not easily identifiable from a single post or image.

35. Mandating an approach that allowed tech companies to moderate users' activity beyond this threshold might encourage a handful of companies to implement and adopt their own assessments of content, with associated punishments. Such an unrepresentative model could have worrying implications for free speech.

36. Nonetheless, there are plenty of measures companies can take to protect their users. For example, Match Group uses an array of proactive safety tools and processes to ensure the safety of our users. These include the automatic scanning of profiles upon creation for red-flag language and images, ongoing scans for fraudulent accounts or messaging activity and manual reviews of suspicious profiles, activity, and user-generated reports.

37. As we are already doing in various jurisdictions around the world, Match Group is willing to work with law enforcement agencies, including the National Crime Agency and police forces, to identify users who have committed criminal offences on our platforms and to pass on their information to the relevant agencies.

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

38. Match Group strives to ensure that its platforms are safe for users, and we undertake regular moderation of profiles to ensure that suspicious profiles are swiftly taken down. We actively encourage our users to report harmful or suspicious accounts. While it is a simple action, this makes our platforms safer for all our communities. We consistently advise our users to be aware of scams, including financial and romance scams, which unfortunately flourished during the initial stages of the pandemic.

39. Given the recent rise in online and romance fraud and the amount of harm it is causing for the victims involved, as well as the persistent threat of fraudulent adverts which are not covered, a greater focus on this from actors across the digital and financial ecosystems is necessary.

40. Match Group therefore welcomes the coverage of scams and fraud in the draft Online Safety Bill but believes there is a necessity to involve actors from the different types of platforms to the app stores, to the marketing platforms and financial institutions, to work together to tackle online scams and fraud.

41. For example, within platforms there is a substantial difference between those platforms who take commission on transactions and those on which money is not involved. This stark difference can influence behaviours and equally require a different approach.

42. As a result, the complexity of online scams and frauds, and the varied range of stakeholders concerned, necessitates a joined-up approach combining data and position within the ecosystem to find and cut off scammers and fraudsters wherever they are identified.

43. However, this challenge is a substantial one, factoring in many sectors, stakeholders, and other existing pieces of legislation. The current approach, which does not yet include fraud within the draft Bill, is unlikely to provide the outcomes that the Plan for Digital Regulation would encourage.

44. Elsewhere, Match Group believes that for the system in which Ofcom is the regulator to work effectively, Ofcom must engage effectively with those entities who are in scope of the Online Safety Bill. Understanding the range of tools and measures in place, the variety across the digital ecosystem and the differing range of remedies required, will benefit Ofcom's future programme of work and fall into line with previous precedents such as the GDPR and privacy by design.

45. Regarding pornography, we suspend accounts that are suspected of selling pornography on our sites and we take swift action to remove these accounts to prevent harm to other users.

What would be a suitable threshold for significant physical or psychological harm, and what would be a suitable way for service providers to determine whether this threshold had been met?

46. Having an explicit definition and process for determining harm would not reflect variation across platforms, brands, and industries, and the constantly changing nature of harms. Different industries are likely to see different issues, and different harms may result from the same behaviour. For example, a 16-year-old interacting with a 40-year-old in the comments section of a news source is very different from a 40-year-old trying to talk to a 16-year-old on social media or a dating app.

47. However, Match Group has recently taken an unprecedented step toward by forming the Match Group Advisory Council (MGAC), a new Board composed of leading experts to help us further maximise the safety of our users. This will help to make the world a safer place for all, and focus on preventing sexual assault, among other offences, across our portfolio. We are willing to share lessons and reflections should this be requested.

Are the definitions in the draft Bill suitable for service providers to accurately identify and reduce the presence of legal but harmful content, whilst preserving the presence of legitimate content?

48. We are heavily invested in the experience of our members and have over 20 years' experience pioneering online dating. We want to attract people to a safe and welcoming place, where meaningful in-person relationships can blossom.

49. We want to ensure that conversation on our platform is safe and respectful, as it would be in real life. We do this through our moderation tools, using both technological and human agents. In this fashion, we can prevent, monitor for, and remove inappropriate, illegal, or harmful content.

50. In practice, this would include acting against content that would be reported to us as 'hate speech', which includes homophobic, racist or misogynistic content. Equally, it could also include fake or 'spam' accounts, or those seeking to perpetrate fraud. In respect of prevention, we also have a number of tools that seek to make members aware of their behaviour before an issue can arise. For example, on match.com, we are deploying an AI tool that can warn a user who is suspected of harassment to make them aware of appropriate behaviour to adopt in their exchanges.

51. Such preventative measures can maintain safety and serve to educate. Should an issue escalate to being reported, we take this incredibly seriously. Reports will be reviewed by a human investigation team trained to deal with such matters and who are able to effectively assess cases. Following this, if the communication is in breach of our terms and conditions laid out publicly for each of our platforms, a user will be banned if the contravention is along the lines of the abuse noted.

52. While our goal is to allow everyone to express themselves freely, it must work alongside our commitment to creating a safe and positive experience for all our users on all our platforms.

The draft Bill sets a threshold for services to be designated as 'Category 1' services. What threshold would be suitable for this?

53. The tech industry is large and varied; with the different types of organisations involved and the varying regulations they are subject to, this means that a one size fits all approach will often fail to achieve its aims.

54. Currently, the categorisation of companies is unclear. We believe that the categorisation of companies by the Bill is most effectively determined by a company's business model. How a business makes its revenue should be used to establish which category it falls under so that it can be grouped alongside similar companies, who are then in turn bound by common rules.

55. For example, Match Group generates the overwhelming majority of its revenue from our member subscriptions. Accordingly, we are heavily incentivised to act in a way that enhances their consumer experience of our service, as opposed to appeasing third parties. Conversely, other organisations that are funded to varying degrees through the amount of data they collect or sell from their users are encouraged to act in a way that might incentivise data collection above consumer interests, for example.

56. As it stands, the vague nature of the Bill as to how the categorisation would be applied is unclear and would appear to group together companies with vastly different business models and, importantly, corporate aims. Fundamental differences include:
    a. The online dating platforms and services that Match Group operates are largely closed networks, where users interact on a peer-to-peer 1:1 basis; this contrasts with traditional social media platforms such as Facebook or Twitter.
    b. It is important to stress that Match Group's business model does not rely on data monetisation / targeted advertising, but on subscriptions paid for directly by users. We only collect and process the data necessary to provide the best user experience. Since we do not sell user data, collecting such unnecessary or unrelated data is not in our business interest and does not add value to the user experience. Match has made a global, company-wide commitment not to sell or share our users' data to third parties for commercial gain, and we proudly stand behind that decision.
    c. Furthermore, the aim of our business model is to reduce online dependency, meaning we want users to move away from online connections to offline in-person relationships. In contrast, other businesses are trying to move more of people's time online to support revenue streams like advertisements and data harvesting. This fundamental difference necessitates a more nuanced approach and greater clarity now that reflects this could help deliver more effectively targeted legislation.

Is Ofcom suitable for and capable of undertaking the role proposed for it in the draft Bill?

57. Match Group understands the difficulty and significant financial cost of establishing a new regulatory body, and it therefore makes sense to designate Ofcom as the regulator. We commit to working closely with them to develop the new Codes of Practice.

58. However, the onus upon the role and direction making role of Ofcom creates a great deal of uncertainty for companies seeking to plan and operationalise any new

regulations. While Ofcom's role as an effective regulator is not in doubt, creating Codes of Practice is a sizeable body of work, as will be the responsibility of companies to comply with those practices.

59. We would suggest that Ofcom could engage closely with other regulators, including the Financial Conduct Authority and the Competition and Markets Authority, to see what frameworks they have in place, and to ascertain from them what works and what does not.

Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

60. Match Group have confidence in Ofcom to deliver a regime that will not prove to be burdensome for its members. However, we would propose that within Ofcom, there should be a Head of Internet Safety reporting directly to the Chief Executive. This would send a powerful signal that Ofcom takes its responsibilities as the regulator seriously and will be seeking to uphold the best possible standards to ensure users are safe online. Simultaneously, Ofcom should continue to increase its headcount to accommodate what will be a substantial new brief. We believe Ofcom is cognisant of this and seeking to deliver accordingly.

How does the draft Bill differ to online safety legislation in other countries (eg. Australia, Canada, Germany, Ireland, and the EU Digital Services Act) and what lessons can be learnt?

61. The draft Online Safety Bill provides the outline of an effective piece of legislation that balances safety concerns with essential rights to privacy. However, some areas of the Bill could be developed to better reflect best case examples elsewhere.

62. The best comparative example would be the EU's Digital Services Act (DSA). The Act will include obligations to introduce measures to combat illegal content online and effective safeguards for users. There are also obligations on large platforms to prevent abuse on their platforms by taking risk-based actions.

63. In practice this means companies with a bigger platform and audience are more liable to sanctions if their platform plays an active role in allowing illegal content to spread. This approach, which recognises the ability to post and share amongst what is potentially millions, is very different from one-to-one messaging networks.

64. Presently, the draft Online Safety Bill does not make this distinction. Given the variety of the digital sector, from social media platforms, to e-commerce, to online dating, consideration of the differing ability of companies to propagate and fuel illegal content is critical in ensuring behaviour change is effectively targeted at and delivered by the tech companies who have been the most consistent offenders.

65. The DSA imposes different sets of obligations for distinct categories of online intermediaries according to their role, size, and impact in the online ecosystem. The categories are as follows:

    a. *Intermediary service*s; provided by network infrastructure providers, including 'mere conduit services' (e.g. internet access) and 'caching services' (e.g. automatic, intermediate, and temporary storage of information)

b. *Hosting services;* provided by providers storing and disseminating information to the public, such as cloud and webhosting services

c. *Online platform services*; by providers bringing together sellers and consumers, such as online marketplaces, app stores, collaborative economy platforms and social media platforms

d. *Very large online platforms (or VLOP) services*; provided by platforms that have a particular impact on the economy and society and pose risks in the dissemination of illegal content and societal harms. Specific rules are set out for platforms that reach more than 45 million active recipients in the EU monthly.

66. The Government could learn from this example of categorisation and apply something similar to the Online Safety Bill, providing more clarity and recognition of the enormity and variety within the digital ecosystem. Not only do different companies and organisations have different roles and functions but their aims can vary wildly, necessitating different approaches to ensure remedies achieve their stated aims.

67. As with the element of categorisation, the DSA provides more clarity on the topic. It states that Member States will have to designate independent digital services coordinators who will be granted specific oversight powers, will be entitled to receive complaints against providers of intermediary services, will have to cooperate with digital services coordinators of other Member States and will be able to take part in joint investigations. A European Board for Digital Services (EDPB) was also set up to ensure effective coordination and consistent application of the new legislation.