Your response

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.

Is this a confidential response? (select as appropriate)

No

Match Group operates a portfolio of adult-only 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 (Group official website: http://mtch.com), including in the United Kingdom where some of our main brands are widely used.

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 networks enabling one-to-many communication, nor do they rely on selling targeted advertising to make money: 98% of our revenues come from subscriptions paid by users.

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.

We are grateful for the opportunity to respond to this consultation. As part of our longstanding commitment to online safety, Match Group has been pleased to support Ofcom and other regulatory authorities, such as the Competition and Markets Authority and the Information Commissioner, with transparency and conscientiousness.

We hope to assist where we can by providing Ofcom with evidence and testimony from our perspective as a medium-sized online service provider. We recently responded to your call for views on the first stage of your online regulation in September 2022, and outline in this response our views on the second phase of online regulation.

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

Is this a confidential response? (select as appropriate)

No

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

The number of smartphones and tablets connecting to the internet (via mobile web or applications) has continued to grow and today accounts globally for more than half of all internet connections worldwide, compared to traditional websites. According to a report by the World Advertising Research Center (WARC), using data from mobile, **more than half of the internet users** (2 billion people) nowadays **only access the web through smartphones and tablets** (and therefore apps), and we expect almost three quarters (72,6%) of internet users will access the web solely via their smartphones by 2025, equivalent to nearly 3.7 billion people.

At Match Group, where all our online dating platforms (Tinder, Hinge, OK Cupid, Plenty of Fish, Meetic, etc.) are 18+, on average more than 70% of our users will access our platforms through smartphones and tablets. This figure rises to 98% for Tinder and 100% for Hinge.

Given these trends, it is clear that many minors are accessing the internet via apps on smartphones, on which they spend almost 3 hours a day on average. This means that services that distribute and advertise apps on smartphones (app markets) will facilitate access to apps for those under the age of 18. Without the correct age-gating procedures in place at the distribution level, underage users are free to download almost any app, including those that have been reserved for adults by app developers.

Apple and Google, through the Apple App Store and the Google Play Store, govern the installation of virtually any app by any user across the world. This fact was recently reaffirmed by an investigation into Apple and Google's anti-competitive practices by the UK's independent regulator, the Competition and Markets Authority (CMA). Indeed, Apple exercises a 100% monopoly on the sale and distribution of apps on their iOS software and Google exercises a similar level of control over Android apps.

Apple and Google are aware that global developments in the digital ecosystem are drawing unprecedented levels of underage users to their App stores. An app store is defined as a digital marketplace that enables users to download apps created by various developers, including those other than the app store's developers, and serves as a storefront allowing users to search and browse for apps. As the providers of these app stores, Apple and Google have the technical ability to prevent minors from accessing certain applications reserved for adults, as evidenced by the existence of parental control functions on their operating systems and their corresponding app stores. In practice, however, when a minor attempts to download an application reserved for adults, a simple prevention pop-up appears on the screen. This pop-up does not block access: a simple click on "ok" allows the application to be downloaded. Meanwhile, app developers must wait for first time users signing into their platforms to trigger their own safety checks.

App stores often not only permit children to download adult-only apps, but they go as far as to encourage it. As observed by the ICO, several adult-only apps are advertised on the app store as 17+ when their developers have repeatedly reaffirmed that no users under the age of 18 are allowed to use their services. This green light misleadingly attracts children to apps that are designed for adults, with potentially harmful consequences. Requests from developers to Apple and Google to correct this glaring discrepancy have repeatedly fallen on deaf ears. Since underage users are required to use an app store and not necessarily download an app, app stores, which are referred to as storefronts by the Government, must acknowledge and respond to this reality appropriately.

Question 3: What information do services have about the age of users on different platforms (including children)?

Is this a confidential response? (select as appropriate)

No

Match Group takes its responsibilities relating to child safety and protection very seriously and has a longstanding commitment to ensure that group platforms do not allow underage individuals to create and maintain an online profile. By preventing access to our platforms, we can help attempt to prevent instances of grooming and related harm to children. Match Group delivers this aim through the combination of technology and human resources, working diligently to keep underage users off of our platforms. In addition to using sophisticated artificial intelligence, our brands collect birthdates, phone numbers, pictures, bios, and other inputs used to assess age, as well as check 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.

However, currently, the first checks are carried out by developers “blind” because each application – whether developed by start-ups or major corporates – is at the end of the internet supply chain. In practice, app developers are forced to wait for first time users signing into their platforms to trigger safety checks in a situation where app stores already hold much more detailed information on a user that can be used to confirm they are who they say they are.

To prevent minors from accessing adult-only apps, the most efficient measure would be to check users’ ages during the distribution step, which means directly in the app store or on the web browser. Importantly, this can be done without the developer knowing their specific age. The simplest way to do this without threatening data privacy would be to force app stores to send a signal (token) to app developers containing the minimum amount of age information: whether the user is below or above 18 years old. This would protect children’s privacy to the greatest extent possible while ensuring that developers can detect and remove underage users from their services when such a service is adult-only.

Match Group has previously requested that Apple prevent underage users from downloading our apps. To date, they have chosen not to do this. However, to reach the next level in our endeavour to tackle online fraud and improve online safety, we need the cooperation of all actors within the digital ecosystem, including app stores such as Apple’s App Store and Google Play Store.

Implementing an age-verification system at the distribution layer of the internet, particularly at the app store level, using anonymised tokens to share age information with developers, is the most comprehensive and swiftest way to protect underage users across the internet, and would set a precedent for other governments to follow, while simply imposing an age-verification mandate on a specific industry falls short of addressing the issue. App stores already hold necessary age information which, as an anonymized token, should be shared from distributors to developers to detect and prevent underage users from accessing age-inappropriate materials.

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

No

The most efficient approach to support services in not allowing children on their platforms is to engage all actors across the digital ecosystem in a holistic way.

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 – our services are for 18 years of age and older and it is right to focus our efforts on protecting children first. We recognise our responsibility as a service provider to shape the regulatory environment for the benefit of all users, not just our own. We believe it is important that all companies within the digital ecosystem adopt a similar approach and take their responsibility seriously.

One way to improve safety for the whole of the online community is to address the issue holistically, importantly making sure that both app developers and the companies that distribute apps (app stores) do more to ensure that children are appropriately kept away from adult applications and content.

However, despite our efforts to detect and remove underage users from our platforms, we require the good will and collaboration of all elements of the digital economy, including the distribution layer of the digital economy: application stores. Apple and Google are the two primary means of app distribution for the vast majority of users – through the Apple App Store and Google Play Store, almost 98% of our members access our services. Yet despite our insistence that our services are for 18 years and above, and our requests for app stores to deny underage users' entry from within the stores themselves, Apple and Google have refused to do this.

To fix this problem, online services (including Match Group) would benefit from the comprehensive regulation of 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. App stores currently play no role in promoting or enhancing online safety, and they are not subject to any duties within the Bill. From our own experience, they have not assisted us in ensuring that as many children as possible cannot access our services.

We are not advocating for less responsibility for the providers of user-to-user services, and we do not intend to shirk our responsibilities to our users. In fact, we hope to be truly world-leading in innovative, robust, and transparent online safety features, promoting best practices in trust and safety that other dating services and online services can emulate.

We will, of course, continue to do our part in taking responsibility for the services we provide and the members we have a duty towards. 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. The policies that Match Group currently have in place provide a solid foundation on which to tackle online harms within Match Group and across its digital ecosystems:

Age gate on all platforms

Question 4: How can services ensure that children cannot access a service, or a part of it?

- With the combination of technology and human resources, we keep underage users off our platforms using AI, birthdate, phone numbers, pictures, bios, and check profiles for red flags. Users are required to enter their age before they can access the website, in a manner similar to age gates used by other age-restricted products, to show they are over 18.

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, including as new content is uploaded.
- The moderation process led by our Customer Care 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 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.

However, we believe that our existing trust and safety measures would be much more effective if there were a concerted effort by *all* elements of the digital economy to do more to protect children. The only way to improve safety for the whole of the online community is to address the issue holistically, importantly making sure that both app developers and the companies that distribute apps (app stores) do more to ensure that children are appropriately kept away from adult applications and content.

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Is this a confidential response? (select as appropriate)

No

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Match Group is proud to be an industry leader in online safety, and we invest millions of dollars and thousands of hours into our trust and safety features, with $125 million going towards our content moderation and user safety features in the last year. Safety is a top priority for us, and we encourage our users to immediately report any behaviour that violates our policies or terms of guidelines. We view our guidelines and policies as dynamic principles which are constantly being assessed and updated to best reflect the evolution of the online experience and needs of our users.

We only provide services for adult users (18 years and older), but our reporting mechanisms and feedback systems we have outlined above are designed for all of our users and are universally accessible to them.

We do, however, take specific measures to ensure that children are not using our platform and that our users can report an underage user if they access the platform in violation of our Terms of Service. These include both human and AI-assisted tools to detect underage users and remove them from the platform as quickly as possible. We have outlined these measures above.

Our safety features use a combination of machine learning and automation, and human oversight and moderation, to ensure the best results and a constantly adapting approach to trust and safety. For example, on one of our most popular platforms, Tinder, we use machine learning to moderate private messages and detect and flag things that are potentially harmful or inappropriate. In Tinder's specific context, individual preferences and other factors can affect how a comment is intended or received in a way that machine learning cannot always detect. The tool was therefore designed to first ask the recipient if they perceive a flagged message to be inappropriate, including if they suspect the sender to be underage, and to direct the user to report it if so. This measure also incorporates user feedback in the moderation process as content reported as inappropriate is, after being confirmed by a moderator, used to further refine the tools.

From this, we've gained valuable insight about what may constitute offensive, harmful or inappropriate content. This has assisted in the development of new prompts; for instance, Tinder and Match have recently implemented a feature whereby senders are prompted to consider whether their message might be perceived as inappropriate or harmful before they even send them.

All of our brands have the ability for users to make a report in-app or contact our customer service team. 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 user accounts across the Match Group portfolio to minimise the risk of potential harm to our other users.

- 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 user "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 user 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 'Match.com' we seek to shape user behaviour, helping them to feel safe and empowered by encouraging reporting. We identify patterns of user behaviour that

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

> might suggest misconduct - for example, when a user 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 moderators can review and take enforcement action where appropriate.

We are proud of the efforts we make every year to put safety at the heart of our services, and we are proud to lead the online dating industry in this regard. Our commitment will not change. However, as we have outlined above, there are other concrete measures which can be taken at other layers of the digital economy to ensure that as many children are protected as possible throughout the digital supply chain and that developers are better enabled to enact their existing trust and safety features. In our experience, many developers want to do the right thing and improve protections for children but lack the collaboration of other elements of the digital economy to make this a reality. Using the data and resources they already possess, app stores can and must do more to help age gate when underage users who try to download apps intended for older audiences.

We will continue to do our part as the developer of our services and as a leading voice for trust and safety in the industry, but we also call on other actors at the distribution layer to do their part. Holistic regulation and responsibility being equally acknowledged across the digital economy will ensure that the online safety regime is as effective as possible. It is time we all have some "skin in the game" to protect users and our children.

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Is this a confidential response? (select as appropriate)

No

We have been clear in our previous evidence to Ofcom that all elements of the digital economy can and must do more to protect children from it. Our services are strictly for those aged 18 and over and we invest meaningful resources, both in terms of capital and human resources, with the aim of providing a safe user experience, which is why we are firm in our stance that one child accessing our services is one too many. Not only we do our utmost to prevent this through a range of trust and safety measures which we have already outlined, but we support the fair application of child duties under the Online Safety Bill to app stores. We believe that more can and must be done at the distribution layer to assist app developers in preventing children from accessing adult services. Given the focus on search services, the role of app stores, defined by the Government's *Code of practice for app store operators and app developers* as "storefronts that allow users to browse for apps, such as via search functionality", is directly relevant to the focus of this question.

The risks of minors accessing inappropriate content through app stores are abundant and deeply concerning. They can be psychological, including when young people are exposed to inappropriate content such as pornography, video game violence or harassment. All of these risks can arise if an app store distributes adult content to a child user and enables

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

interactions between children and adults, especially when they already have the data to determine that the user is underage but they refuse to act.

Several studies have pointed out app stores' failings in safeguarding children online. 5Rights, a children's digital rights charity, submitted concerning evidence to the Information Commissioner's Office (ICO), demonstrating how an Apple iCloud account registered to a 15-year-old child was able to download 16 online dating apps by 'simply by tapping 'OK' to confirm we were over the required age'. In their letter to the ICO, 5Rights concluded:

> *'Many services with age restrictions are advertised on the Apple App and Google Play stores as child-friendly, suitable for users of any age or ages younger than those specified in the service's published terms. The app stores also allows accounts registered as children to download age-restricted apps with little or no friction'.*

Their conclusions mirrored those of the Tech Transparency Project (TTP), which conducted a similar study in 2021 and found that the 'underage user could easily evade age restrictions in the vast majority of cases', exposing them to apps such as 'Eros: Hook Up & Adult Chat' and 'KinkD: Kink, BDSM Dating Life'.

Indeed, as 5Rights states, app stores often not only permit children to download adult-only apps, but they go as far as to encourage it. As observed by the ICO, several adult-only apps are advertised on the app store as 17+ when their developers have repeatedly reaffirmed that no users under the age of 18 are allowed to use their services. Requests from developers to Apple and Google to correct this glaring discrepancy have repeatedly fallen on deaf ears.

Additionally, the age rating for an app is determined arbitrarily by the app store, and developers have no say in the matter. For instance, an app designed exclusively for adult users can be advertised as suitable for 17+ users, despite the developer's insistence that it is only meant for 18+ users. For example, the 5Rights Foundation stated it found 12 "systemic" breaches of the Age Appropriate Design Code, including insufficient age assurance; misadvertisement of minimum ages for games on app stores; the use of dark patterns and nudges; data-driven recommendations that create risks for children; a routine failure to enforce community standards; low default privacy settings; and more. This issue was subsequently acknowledged by the ICO in their research.

Meanwhile, researchers at the International Computer Science Institute at the University of California, Berkeley, found that more than half of 5885 child-directed Android apps that are included in Google's Designed for Families programme potentially violated the US Children's Online Privacy Protection Act (COPPA).

The evidence raised by research groups, children's charities and independent regulators are telling of Apple and Google's failure to take responsibility for children's safety online. This contradicts both companies' stated commitments to protect of all of their users from 'bad actors or harmful consequences online' – a pledge that has already has its veracity challenged by the Competition and Markets Authority.

The failings of app stores to appropriately fulfil their obligations towards child users results in direct and widespread risks to millions of underage users, who are forced to use one of

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

only two app stores (the Apple App Store and Google Play Store) to access content and services on their devices. Because of this risk, we advocate for the fair and equal application of child protection duties to app stores under the new online safety regime.

Contrasting the lack of co-operation from those at the distribution layer, Match Group takes its responsibilities relating to child safety and protection very seriously and has a longstanding commitment to ensure that group platforms do not allow underage individuals to create and maintain an online profile. By preventing access to our platforms, we can help attempt to prevent instances of grooming and related harm to children. Match Group delivers this aim through the combination of technology and human resources, working diligently to keep underage users off of our platforms. We also utilize technology and humans in combination beyond the registration stage to look for and report newly created Child Sexual Abuse Material (CSAM) or other content that may be harmful to children.

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Please see our answer in question 6.

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

[Please select]

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Is this a confidential response? (select as appropriate)

No

One risk factor which has been overlooked is the vast influence of distribution platforms upon children accessing content which could be harmful to them. As we have noted above, more than half of the internet users (2bn people) access the web through smartphones and tablets (and therefore Apps). This is a high level of market dominance which should be matched by a sufficient level of responsibility for child protection. App stores have an overwhelming level of reach and influence in the digital economy, and their inaction on child safety is glaring.

The risk, therefore, presented by the inaction of app distribution platforms is enormous, and has not been addressed thus far in the UK's online safety debate. When the largest distributors of online content have not implemented sufficient age controls for adult services in their stores, this exposes millions of children to the potential harm of downloading an adult service.

Our proposal for a greater level of protections at the distribution layer directly addresses this risk. If children are sufficiently prevented from accessing adult services, they are pre-emptively protected from a myriad of potential online harms, thereby reducing risk. This risk is reduced for an enormous number of users, app stores have a huge obligation to assess the risk on their platforms and act accordingly to mitigate that risk. Their responsibility is the same as any other service provider. By mandating action by app stores, responsibility is not diminished elsewhere in the digital ecosystem. Instead, all actors are committed to working together in the interests of children and adult users. We will continue to advocate for this fair and reasonable attitude of equal treatment.

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

Is this a confidential response? (select as appropriate)

No

Match Group's safety policies demonstrate what we can achieve with a thoughtful, dynamic blending of human resources combined with industry leading technology. Through iterative processes and innovative strategies, we continually improve upon our existing trust and safety features to ensure that we are an industry leader for best practices in protecting our users.

We also work with industry-leading NGOs that serve on our first-of-its-kind Advisory Council established in 2018, we draw upon the collective expertise of our users, multiple internal departments, and external experts to create our policy guidelines and safety features. The Match Group Advisory Council includes experts and advocates involved in the study and prevention of sexual violence and harassment, sex trafficking and similar issues.

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

We are a provider of adult-only services. Our view is that children should not be on our platform whatsoever – in that regard, all of our efforts regarding child safety are devoted to detecting underage users on our services and removing them from our services.

To keep underage users off adult Match Group platforms, we:

- Ask registering users to input their date of birth to indicate their age, which 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 (Apple and Google, however, do list our brands, including Tinder as +17 apps, despite our long-standing requests for these to be listed as an 18+ app);
- Scan user's profile pictures using automated tools to estimate the age and all flagged pictures are double-checked by a human moderator (our photo moderation flagging system deliberately relies on a high rate of false positives) which are then checked by human moderation to ensure appropriate action is taken; and
- Actively monitor our platforms through a combination of technology and human moderators to detect suspicious profiles and take swift action to remove them. We also rely on other users to report suspicious or concerning profiles.

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. We spent more than $125 million last year alone on product, technology and moderation efforts related to trust and safety to prevent, monitor and remove inappropriate, illegal, or harmful content.

We understand the potential impact of our services on our members and recognise the value of the user voice through feedback and human monitoring, drawing upon the valuable insight and experiences of our users to make our services better. Technological improvements are enhanced and maintained through the hiring and continuous training of our Security, Trust and Safety, Customer Care and Moderation teams. We intend to continue innovating with our governance and trust and safety features to promote our best practices in online dating and beyond.

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

Is this a confidential response? (select as appropriate)

No

Our platforms are not designed for children, and therefore we prioritise safeguarding children by focusing on identifying underage users on our platform and implementing measures to prevent their access to our services.

We have also detailed above how we detect and remove underage users from our platforms, as well as our recommendations on how the entire digital economy can holistically work

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

together to remove children from adult services and improve the efficacy of existing policies and measures.

It is unlikely that children will read Terms of Service, and it is well-known that children can and do attempt to circumvent age assurance measures through VPNs, false information and other means. However, an effective age-gating solution at the distribution layer would address these issues by allowing developers to block underage users from their platforms while providing clear reasoning for their removal from the service.

As a service provider, we provide clear, easy-to-read statements on our policies and make it clear that we do not allow children to access our services. We follow this guidance with firm action, removing any underage user from our services as soon as possible. We would, however, be assisted in our goals through the cooperation of the distribution layer, and we ask that app stores play their role in the new online safety regime. For example, listing apps as "17+" when they are clearly for 18 and over, and a request has been made by the developer of the app store to this effect, creates a totally unnecessary confusion and is not consistent with UK age ratings.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[1]

Is this a confidential response? (select as appropriate)

No

Our platforms are for adults only and our Terms of Service specifically prohibit minors from registering on our services. These terms of service are reviewed periodically by our brand lawyers, in consultation with our Product and Trust & Safety teams.

We also prohibit the use of all of our services for illegal or harmful purposes, with additional restrictions regarding what we deem to constitute illegal content or harmful conduct specifically as to our services. When we suspend a user for violating these terms and conditions, we provide an explanation that they do constitute a material breach and explain the consequences of such actions clearly and plainly. We remove such users from the platform and potentially (depending on the severity of the illegal act or content) from all other platforms across the Match Group's portfolio, therefore affecting current and future registrations. This is intended to protect as many of our members as possible from exposure to harmful material.

Generally, we see very little Illegal content on our platforms which would be considered 'primary priority content' in the new UK online safety regime. Of the users we have removed from our platforms, very few are removed based on primary priority or priority content such as terrorism or Child Sexual Abuse Material (CSAM) content. As noted above, our platforms are mainly closed networks enabling private, peer-to-peer communications between adults and generally our platforms are not open social networks enabling one-to-many

[1] See A1.2 to A1.3 of the call for evidence for more information on the indicative list of harms to children.

Question 12: How do terms of service or public policy statements treat ‘primary priority’ and ‘priority’ harmful content?[1]

communication, which makes the dissemination of illegal content using our services ineffective and limited.

If something is illegal offline, it has no place on our platforms, and is removed by our teams as quickly as possible. Platforms are alerted of potentially inappropriate or harmful user accounts or content, including racist and terrorist content, by a combination of automated tools and user generated reports. All user generated reports are reviewed and acted on appropriately and we actively encourage our users to be vocal and active in reporting content they find upsetting or inappropriate.

In addition to these measures, Match Group has a long history of working in partnership with women-focused organisations including the National Sexual Violence Resource Center, Thorn, RAINN and the MeToo movement, amongst others, to raise awareness of the Group’s focus and efforts to prevent sexual assault, sex trafficking, abuse, harassment, and similar issues.

Our AI tools are crucial to ensure the effective implementation of our terms of service. Match Group’s AI tool has three main objectives:

1. Proactively engaging users if behaviour relating to a form of harassment is detected
2. Providing support for the harassed user, including through a reporting function
3. Warning the user who is suspected of harassment and making them aware of appropriate behaviour to adopt in their exchanges or banning them if the behaviour is indeed serious enough.

We are currently undergoing updates to our categorization and tracking of safety-related data and look forward to sharing more on this in the future in compliance with pending Transparency Reporting requirements under the Online Safety Bill.

In addition to our terms of service, Match Group services also have Community Guidelines (see, e.g., Tinder’s Community Guidelines) and Safety Tips (Tinder Safety). The Community Guidelines and Safety Tips are written in an easy-to-use, conversational style that is clearer and more accessible to our users, as it is written as a direct communication to them rather than in contractual terms necessary for the terms of service. These are available to users in prominent positions on our platforms.

We also aim to empower our users through user-friendly feedback to maximise safety and understanding while improving understanding of our terms and services. In certain cases where users have been found to be in breach of the organisation’s community guidelines for a relatively minor offence, our brands have implemented a strike system whereby instead of immediately banning a user, we issue a strike or warning against them and offer opportunities for feedback. For instance, offering private information in a biography is not allowed under our brands’ Community Guidelines but the user may not realise this, so we offer information about the reason for the strike and explain to the user where they have gone wrong.

In offering users opportunities to become more informed about infractions of rules, we provide a more equitable pathway to improve the safety of users, delegating agency to users, and cultivating a sense of responsibility that allows users to align their behaviour with other users’ expectations before more severe enforcement action is required. We

Question 12: How do terms of service or public policy statements treat ‘primary priority’ and ‘priority’ harmful content?[1]

have found a significant degree of success in this strategy, having seen very low rates of recidivism and a significant reduction in bans.

Question 13: What can providers of online services do to enhance children’s accessibility and awareness of reporting and complaints mechanisms?

Is this a confidential response? (select as appropriate)

No

Safety is a top priority for us, and we encourage our users to immediately report any behaviour that violates our policies or terms of guidelines. We view our guidelines and policies as dynamic principles which are constantly being assessed and updated to best reflect the evolution of the online experience and needs of our users.

The reporting mechanisms and feedback systems we have outlined above are designed for all our users and are universally accessible to them. However, as we only provide services for adult users (18 years and above) we do not intentionally design user reporting and complaints systems to be child-friendly or accessible to children.

We do, however, take specific measures to ensure that children are not using our platform and that our users can report an underage user if they access the platform in violation of our Terms of Service. These measures include both human and AI-assisted tools to detect underage users and remove them from the platform as quickly as possible. We have outlined those measures above and we will provide further detail of our blend of human and AI safety tools below.

Our safety features use a combination of machine learning and automation, and human oversight and moderation, to detect underage users for removal. This blend of human and machine tools helps to ensure the best results and a constantly adapting approach to trust and safety. For example, on one of our most popular platforms, Tinder, we use machine learning to moderate private messages and detect and flag things that are potentially harmful or inappropriate. Human moderation is then used to further refine these machine-assisted tools as well as to appropriately account for tone, context and other factors which AI tools might miss or misinterpret.

To give an example, if a user tells another user, “I’m only fifteen”, our machine learning tools will identify this and report it to our human moderators, who will assess the veracity of the flagged message before taking appropriate action by removing the child. When a child is removed from our services, they are informed of the reason for their removal and prevented from accessing our portfolio of online dating services until they are adults.

From this mixed-method approach of human and machine tools, we’ve gained valuable insight about what may constitute offensive or harmful content. This has assisted in the development of new prompts; for instance, Tinder and Match have recently implemented a feature whereby senders are prompted to consider whether their message might be

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

perceived as inappropriate or harmful before they even send them ('Are you sure?'). This incentivises the user to think before they send and promotes better behaviour on our service before disciplinary action is necessary.

All of our brands have the ability for users to make a report in-app or contact our customer service team. 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 user accounts across the Match Group portfolio to minimise the risk of potential harm to our other users.

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

Is this a confidential response? (select as appropriate)

No

As Match Group services are strictly for users over 18, we do not believe we are best placed to advise Ofcom on legal content which is harmful to children. Our one-to-one messaging services, which limit the virality and exposure of potentially harmful content, as well as our zero-tolerance policy for children on our platforms, mean that we do not design and maintain specific processes to account for children being exposed to other users' legal but harmful content. We have noted above that our efforts to protect children focus on keeping them off Match Group services.

As we have noted above, our Terms of Service and our reporting and complaints mechanisms are universal and easily accessible to all our users, and we encourage proactive engagement with our moderators to provide the safest and most enjoyable experience on our platforms. This would also apply to a child who encounters harmful content on our platforms as it would for any other adult user. However, the child being on our service is a direct violation of our Terms of Service and would be removed as soon as they were detected.

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Is this a confidential response? (select as appropriate)

[Please select]

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Is this a confidential response? (select as appropriate)

[Please select]

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

Is this a confidential response? (select as appropriate)

[Please select]

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Is this a confidential response? (select as appropriate)

[Please select]

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?

Is this a confidential response? (select as appropriate)

No

Match Group services do not employ algorithms which have any direct impact on child users, such as recommending content to children as other platforms might do. Because our services are adult-only, one-to-one messaging services, the structure of our business model and the functions of our services are very different and are explicitly not meant to be accessed by children.

However, we are aware that there is a broader question about how algorithms and advertising affect children in the digital marketplace. For our business, we are concerned that some of our services, such as Tinder, are advertised within app stores such as the Apple App Store as “17+” rather than 18+, which therefore directly advertises the service to underage users (17-year-olds) despite our strict Terms of Service and explicit policies about underage users.

This issue of how our services are advertised has not yet been addressed. Despite numerous requests to the parent companies of these app stores, our services are still not advertised as 18+ only. This directly incentivises under-18s to access our services in violation of our policies. We have no control over how our services are age-rated within the store, and app stores take no active measures to ensure that those under the specified age cannot access the service. We request that app stores do their part in advertising adult services appropriately to adults only and blocking underage users from accessing such services by anonymising and sharing the required age information.

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Is this a confidential response? (select as appropriate)

No

One aspect of content moderation which is overlooked is how services (and thereby the content within those services) are advertised to potential users by consumers. To give an example, our online dating service, Tinder, is listed on Apple's App Store as an app for users who are "17+", despite our firm insistence that the service is for 18+ only. As 17-year-olds are not adults, the listing of our app as "17+" actively incentivises under-age users to access our platform.

As we have previously noted to Ofcom, the incorrect age rating of our apps at the distribution layer of the digital economy is directly counteracting our own wishes as the developer of the service. We dedicate hundreds of millions of dollars and many hours into online safety features each year, yet we have no control over how our services are inappropriately advertised to users who would violate our terms of service by accessing our platforms underage. We have received no assistance from Apple or other app distributors on this matter, despite numerous requests over an extended period.

Requiring app stores to appropriately list adult-only applications (as defined by the service developer themselves) would be a cost-less measure which would undoubtedly prevent more children from accessing the service without unduly restricting their user activity.

As we have previously noted, app stores already hold the necessary age information to detect underage users. We have similarly been explicit in our Terms of Service and our correspondence with app distributors that our services are 18+ only. There is a clear, logical and zero-cost solution which is ready to be implemented. We believe that Ofcom, as the rightful regulator of the UK's online safety regime, should be able to enforce these holistic standards.

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

For Match Group, the profitability of our services and the safety of our users are directly intertwined. This is because our business model relies on providing an experience that is valuable enough that our customers want to purchase subscriptions such as Tinder Gold. Users will only consider subscribing to an online dating service if they are enjoying the service. We are intent on providing a safe and enjoyable experience for adults which exposes them to legal content only, and our business model and existing trust and safety efforts reflect this. These moderation systems are designed for adult users, not children – children are not meant to be on our services whatsoever.

For us, therefore, it is imperative that we provide a safe and enjoyable experience, and we employ both human and technological safeguards to ensure this. A foundational point of our

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

efforts in trust and safety is that our services are adult-only. The presence of minors on our services presents a danger to the safety and enjoyment of that experience, as users do not want to interact with a child on the service, and they will not subscribe if they encounter children on the platform. For that reason, we are strict in the enforcement of our Terms of Service and remove underage users from our platform immediately. This is the cornerstone of our investment into trust and safety: keeping children safe by keeping them off the platform, keeping our users safe, and providing an enjoyable experience by ensuring that the adult service is free of any underage users.

We incorporate a PhotoDNA review for known CSAM which works to reduce illegal content from ever making it to be seen by our users. We also utilize technology and humans in combination to look for and report newly created CSAM or other content that may be harmful to children. Similarly, we have significant rules around bots, spams, and attempted scammers, where we are constantly blocking actors looking to take advantage of our users. We also scan messages for problematic phrases which are consistently used in the violation of our Terms of Service, relating to terrorist content, CSAM, illegal substances and other illegal content which is not welcome on our platform. Our one-to-one messaging platforms are not end-to-end encrypted - the scanning of user messages is conducted to ensure the safest possible experience for our users.

Again, we stress that these moderation systems are not specifically designed for content which is harmful to children, instead they are designed to keep children off our platforms in line with our Terms of Service. However, our moderation systems are also designed for content which is universally harmful to our users. Fundamentally, we take the utmost care to ensure that children are not able to access the service while leading the industry in providing the safest and most enjoyable experience possible for our users who are of sufficient age to use the service. We also accept that this is an ongoing commitment that requires constant attention, care and investment to ensure that we meet our responsibility as the market leader in this space.

Question 22: How are human moderators used to identify and assess content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

Match Group's safety policies demonstrate what we can achieve with human moderation and online tools. Our platforms use a combination of human review and machine learning and/or automated technology (e.g., programs that can identify nudity and other inappropriate content and photos) to ensure that children are unable to use our services and that legitimate adult users on our services are presented with safe, legal and enjoyable content.

A dedicated community team is responsible for each platform, which a user can directly engage with to report inappropriate content or behaviour. Each platform has trained human agents, whether internal and/or outsourced, that swiftly review and respond to these reported concerns.

Question 22: How are human moderators used to identify and assess content that is harmful to children?

We also flag a random sample of content for review by human moderators looking to identify new and emerging patterns of harm. This casts a wider safety net around the moderation process, ensuring that the majority of content violations are removed before being viewed by users. Human moderation ensures a sufficient level of oversight for our machine-assisted systems to adapt to the rapidly changing online environment, ensuring that violations of our Terms of Service are adequately spotted and addressed while also ensuring that users are able to interact freely on our service when they are not in violation of those Terms of Service.

We provide front-line moderators with the necessary tools to face disturbing content daily, including individual and group counselling sessions; ongoing monitoring and wellness programs; and provision of information and resources. We aim to enable our moderators to better protect our online communities while ensuring our content moderation team itself is well cared for.

To prevent underage users from accessing our services, we incorporate a variety of methods such as age-gating, machine-assisted scanning of messages, PhotoDNA and other tools, which are overseen by human moderators. We are also pleased to work with Ofcom, the UK Government, Parliamentarians and other stakeholders to advance the online safety effort in the UK. We fully support efforts to strengthen the online safety regime and implement it as soon as possible, and we are pleased that Parliament is expressing a strong desire for a robust and holistic online safety regime through amendments to the Online Safety Bill which call for stronger age assurance measures.

Question 23: What training and support is or should be provided to moderators?

Is this a confidential response? (select as appropriate)

[Please select]

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?

Is this a confidential response? (select as appropriate)

[Please select]

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?

Question 25: In what instances is content that is harmful to children, that is in contravention of terms and conditions, removed from a service or the part of a service that children can access?

Is this a confidential response? (select as appropriate)

No

As we have noted, children are not allowed on our platforms and any instance of an underage user is a direct violation of our Terms of Service which is dealt with as soon as possible. Any contravention of our terms that we discover is dealt with either by removing the content in violation of the terms or banning the user. We aim to provide a safe, secure and legal environment for enjoyable interactions between adult users. This is our top priority and we have demonstrated elsewhere how and why we do this.

Question 26: What other mitigations do services currently have to protect children from harmful content?

Is this a confidential response? (select as appropriate)

No

We have made clear here and elsewhere how we continue to invest and innovate in this area given its importance to our commercial aims and company ethos. As we have noted above, Match Group advocates for a larger layer of protections for children and underage users at the distribution layer of the digital economy. The requirement for app stores and other access facilities to share anonymised age information with app developers would provide another means of preventing children from accessing adult services, in addition to the efforts already undertaken by developers, thereby protecting them from potential exposure to online harms and age-inappropriate content.

App stores are the primary access point for more than half of the internet's current user base (more than 2 billion people) and it is estimated that by 2025, 72.6% of internet users will access the internet solely via their smartphones (almost 3.7 billion people). However, app stores currently have no requirement to conduct risk assessments or introduce age assurance measures under the current draft of the Online Safety Bill, despite this huge influence on how users find and access content.

Question 26: What other mitigations do services currently have to protect children from harmful content?

Without specific measures to proactively prevent children from accessing adult materials directly at the point of access (i.e., the download button within the app store), our trust and safety measures will not be sufficient to identify and remove every underage user as early as possible. This is because the developer of the application is forced to conduct checks on users 'blind', without the age information which the stores already hold. We are only able to identify and remove a child from a Match Group platform once they have already downloaded the app, by which point they may have already been exposed to adult content. We have previously expressed these concerns to both Apple and Google, asking them for their help numerous times to enforce our Terms of Service for our services through their store. They have not done so.

A user's age information could be shared with the developer by means of an anonymised token, which would allow the developer to identify a user as 'underage' and block them from the service. Stores already have the age information of their users, both through their Apple ID/Google Account and through third-party validators which store their data on the device itself.

If this information could be shared anonymously with developers, it would simultaneously prevent children from accessing content which is not meant for them, while ensuring the maximal data privacy of those children.

The sharing of anonymised and encrypted age information from distributor to developer could be mandated if Ofcom were able to enforce this upon distribution platforms under Part 3 of the Online Safety Bill in clauses 10 and 11. To this end, Match Group has been supportive of an amendment moved by Baroness Harding and other cross-party Peers in the House of Lords which would subject app stores to the same requirements as other service providers. The fair, logical and reasonable application of duties to all services would ensure that the online safety regime is as robust, consistent and effective as possible, and that children are given an extra layer of protection at the greatest access point in the digital economy.

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

Is this a confidential response? (select as appropriate)

No

As we are clear about our policies regarding underage users, we conduct both human and machine-assisted checks to detect and remove underage users. However, these checks can only be conducted once the user has downloaded and accessed the app.

These checks could be conducted earlier, preventing children from accessing the service and further limiting the risk of harmful content. This would be done at the point where the children access the service – the distribution platform – to intervene and block the underage user as soon as possible.

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

As we have noted, the primary access facility in the existing digital economy is the app store. Over half of existing internet users (including children) access services and content via these app stores, and two companies – Apple and Google – have direct control over which users can access each service, and how each service is advertised to them.

Because app stores do not always prevent underage users from accessing adult-only services, despite where an age is known, we are forced to conduct blind checks on users once the user has accessed the service, without the necessary age information to immediately detect and reject or remove the underage user. We do not receive any assistance from the distributor (the app store), despite the fact that both companies collect this age information and have complete control over which users access which services.

We believe that the inaction of app stores is unacceptable and that their exclusion from the scope of the Online Safety Bill poses a huge barrier to the effective implementation of the new online safety regime. We must all play an equal role in creating a safer environment for children online – a logical step towards this goal must be the effective age-gating of adult services at the distribution layer of the digital economy.

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

As we stated above, we believe that children could be protected more effectively if there was a second layer of protection at the distribution layer of the digital economy, as well as on the service itself. Holding both the service provider and the app distributor or app stores accountable for their work on trust and safety is crucial to the success of the UK's online safety regime. Not only is this logically consistent and fair but will make an enormous improvement for developers who are currently conducting age assurance measures without the age information they need.

The Online Safety Bill's purpose is to deliver a safer online experience. Without the inclusion of app stores, the aims of the Bill cannot be satisfied. Collective responsibility to prevent online harms for children therefore lies with both the developer and app distributor or app store. A holistic approach is fundamental to online safety due to the interconnected mechanisms of how the industry works. Unfortunately, the self-regulation of big tech has failed and a mandated approach is necessary. Without the inclusion of app stores in the Bill, the world's largest companies will not have a proportionate role to play in keeping users safe online.

We believe that our perspective as a medium-sized, adult-only service provider in the UK can provide valuable insights to Ofcom, and we value and appreciate our existing relationship with Ofcom as an independent regulator. We firmly believe that the robustness and integrity of the online safety regime will be best served by a close and collaborative relationship between Ofcom and industry actors, and we are proud to be part of that relationship.

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?

As such, we will continue to offer our perspective on best practices in trust and safety while advocating for positive change which puts user safety and enjoyment at the heart of the online experience. We are grateful to Ofcom for the opportunity to contribute our views to this consultation and to future calls for evidence.