



Match Group’s submission to the development of the Second National Action Plan to End Violence against Women and Children

1. Introduction	1
2. Our Trust and Safety Philosophy	1
3. Measures to Prevent and Respond to Harm	3
4. Engaging with Australian Authorities	4
5. Partnerships and Collaboration	5
6. Access to Sex Offender Registers	5
7. Answers to Questions in the Consultation Paper Relating to Technology Facilitated Abuse and Online Platforms	6
8. Conclusion	8

1. Introduction

Match Group (“Match”) welcomes the opportunity to contribute to the consultation process for the development of the Second Action Plan to support the National Plan to End Violence against Women and Children. We recognise the serious and harmful impacts of technology-facilitated gender-based violence and are pleased to contribute to whole of society efforts to combat this issue.

Match Group is a leading provider of digital technologies designed to help people make meaningful connections. Our portfolio includes Tinder, Hinge, OkCupid, Plenty of Fish, Match.com and Meetic, serving users in more than 186 countries and over 60 languages. Since pioneering online dating, Match Group brands have enabled hundreds of millions of connections across the worldwide.

At the core of our efforts are a fundamental and profound commitment to promoting safety in dating and across the internet. Across Match Group, we are dedicated to fostering inclusive environments where people can connect safely and authentically.

We note the consultation paper raises issues around online platforms and technology facilitated abuse and asks three specific questions around these matters. Our submission outlines how we address these issues within our business, along with a specific suggestion around access to convicted sex offender and potentially domestic violence offender registers which we believe can play a significant role in further improving the safety of users engaged in online dating.

2. Our Trust and Safety Philosophy

Match Group’s dating platforms primarily exist to facilitate private, one-to-one interactions that can lead to offline meetings, creating safety considerations distinct from other internet services or social

media. Match Group designs its products with these risks in mind, recognising that online interactions can, in rare instances, translate into real-world harm.

User safety, both online and off, is fundamental to Match Group's mission to spark meaningful connections. Trust and safety are embedded across our products, policies and operations, with continuous investment in tools, technologies and teams to help people connect with confidence. This includes proactive detection of and enforcement against potential harms at scale – globally, the vast majority of our enforcement actions are taken without the need for a user report, and all of Match Group's apps deploy key proactive safety features such as identity verification, harmful message detection and in-app safety tools.

In Australia, Match Group has played a leading role in advancing industry standards, including through the development of the voluntary [Online Dating Code of Conduct](#) in partnership with government, regulators and other platforms. The Code establishes clear expectations for how services prevent, detect, and respond to harm, and reflects a shared commitment to transparency and accountability.

Match Group also works closely with Australian governments, law enforcement, and NGOs to strengthen safety outcomes, including through user education, reporting mechanisms, and escalation pathways for serious incidents. This collaboration is critical given the scale of activity on our platforms and the evolving nature of online-enabled harm.

Our centralised Trust & Safety department leads this work, along with policy, enforcement, and regulatory engagement across our portfolio. The investments Match Group makes in this function are meaningful: Match Group invests over USD \$125 million annually in trust and safety, enabling us to build innovative safety products and take action against harmful behaviour at scale, including removing hundreds of thousands of accounts in Australia for violating our rules, including abuse, harassment and violence-related conduct.

Match Group's core [Trust and Safety principles](#) are:

- Safety by Design: we focus on proactive integration of safety measures in every phase of the product life cycle. We continuously evaluate and improve existing and new safety features.
- User Control: we build inclusive, welcoming platforms where users are empowered to shape their own dating experience. Match Group apps offer tools that support healthy dating experiences, including profile visibility and contact options and protect against identity-based abuse and harassment.
- Authenticity and Trust: genuine connections start with knowing who you're talking to. Our vision is a platform where every user is verified, and Face Check, our industry-leading biometric verification tool, is how we get there. Face Check validates account uniqueness, confirms a user matches their own photos, and screens out bad actors and duplicate accounts before they can cause harm, all while preserving user privacy. Already mandatory for new users on Tinder and Hinge in Australia, Face Check is central to our push toward 100% verification across our platforms.
- Inclusion: we seek to create inclusive and welcoming platforms for everyone, regardless of their identity, background, or sexual orientation.

3. Measures to Prevent and Respond to Harm

Match Group's safety approach begins with clear and comprehensive policies to address harm — both within our apps and across the broader ecosystem within which we operate. On our apps, we enforce a high bar of safety, often significantly exceeding the content standards common across social media

and other internet platforms: We prohibit hate speech and do not tolerate harassment or abuse on the basis of someone's identity or other protected characteristics, including sexual orientation and gender. Dating needs to be an inclusive and safe experience, and our policies reflect this intention. We also strictly prohibit underage use, prostitution, and sex trafficking, as well as fraud and scam-related activity.

To operationalise these policies, Match Group applies a layered safety approach that combines technology, human review, and user-facing tools. This includes industry-leading verification features such as Face Check™ on Tinder and Hinge —a mandatory video selfie feature introduced in Australia that strengthens identity assurance and has been shown to significantly reduce exposure to bad actors and reports of harmful behaviour. As Face Check becomes mandatory for more of our user base, we are working toward a platform where every active user is verified -- a meaningfully higher bar than the optional or photo-only verification models common elsewhere in the industry. And, across the account lifecycle on our services, we proactively identify, detect, and take action against individuals and networks that violate our policies, including removing accounts and employing advanced systems to help prevent re-entry across our platforms.

We have also built in-product interventions designed to help prevent harm before it occurs. Features like "Are You Sure?" and "Does This Bother You?" use real-time prompts to discourage inappropriate messaging and empower users to report concerning interactions. Across Hinge and Tinder, we offer both user-controlled and AI-powered message and comment filters, to allow users to effectively manage the messages they receive and exclude content that they may view as unwanted or inappropriate. Additionally, all of our largest dating apps in Australia do not allow private sharing of images, a safety-by-design decision which further reduces the possibility of our apps being used to enable critical harms, such as the dissemination of child sexual abuse material or non-consensual intimate imagery. Tools such as "Share My Date," available on Tinder and Plenty of Fish, allow users to share key details with trusted contacts when meeting matches offline. Hinge's "We Met" survey checks in with users after they connect offline. If a user indicates they do not want to meet their match again, they are also offered the option to make a report.

All of these features are backstopped by comprehensive, easy-to-use, and trauma-informed reporting functions. Since 2021, Match Group brands like Tinder, Hinge, OKCupid, and Plenty of Fish have worked closely with global experts, including in Australia, to continuously improve in-app reporting features to ensure users can straightforwardly report experiences of harm, without the need to re-experience traumatic experiences. Among the critical improvements we've made based on feedback from users and experts in Australia is ensuring, across our portfolio, that members can report someone they've unmatched with (or who has unmatched with or blocked them).

Whether reported by a user or identified proactively by our AI systems, we take a hybrid approach to enforcing our trust and safety policies, combining automated adjudication of straightforward harms with escalated human review for more complex issues. In every instance, reports of serious misconduct, including allegations of off-platform harms such as sexual assault, are escalated to dedicated, human reviewers, who are specifically trained in how to approach these matters with sensitivity and nuance. Our approach to sexual misconduct is grounded in three principles: a universal bias towards protecting the safety of our members, procedural fairness in enforcement, and trauma-informed engagement. We have developed internal standards to support consistent evaluation of both first-person and third-person reports — including those made by individuals who may not be app-users themselves. Crucially, if an account is banned as a result of these reviews, enforcement actions are shared across Match Group brands using an advanced cross-brand database that keeps potential bad actors from accessing any of our services, not just the one on which they were reported.

All Match Group brands are intended to be used exclusively by adults over the age of 18, and consequently, our apps operating in Australia use a multi-layered approach to prevent minors from joining the platform. Merely requesting age disclosure is insufficient as a standalone age assurance measure, so we implement multiple layers to ensure better accuracy and deterrence:

- **App store restrictions:** All Match Group apps are rated 18+ for iOS and Android. Properly configured parental controls can effectively prevent minors from downloading or accessing these services. We also adopt emerging tools from the Apple App Store and Google Play Store, as they become available, to block access to our apps in search and prevent transactions from accounts identified by app stores as minors.
- **Age-gating at registration:** On Match Group's dating apps, if a user provides a birthdate indicating they are underage, the account is automatically blocked and prevented from trying again. Users who enter an incorrect birthdate may regain access only through verification with a government-issued photo ID.
- **Image and text-based moderation:** We employ a combination of automated tools and human oversight to detect potential underage users.
- **In-app reporting:** Users can easily report suspected underage profiles for immediate review.
- **Photo ID verification:** Users who are banned or flagged for suspected age violations may appeal by verifying their identity with a valid government-issued photo ID.

Beyond enforcement, Match Group invests in user education and [transparency](#). All Match Group apps include in-product Safety Centres that provide localised resources, guidance and tools to help users make informed decisions. Match Group also publishes [Healthy Dating Guides](#) to support safer interactions from online engagement through to in-person meetings.

Match Group prides itself on our support and cooperation with law enforcement and stands ready to assist in any active investigations. A law enforcement portal has been developed to facilitate valid legal requests for access to data for investigative purposes in a timely fashion, with the overwhelming majority of requests to our brands processed in 24 hours or less.

4. Engaging with Australian Authorities

Match Group maintains strong, constructive relationships with Australian governments, regulators and law enforcement agencies, with a shared goal of improving user safety and strengthening trust in online services. Our approach is grounded in ongoing collaboration, transparency and a willingness to support practical, effective solutions to emerging risks.

Match Group has a productive relationship with the eSafety Commissioner and her office, reflecting a shared commitment to user safety and responsible industry practices. Match Group also works closely with the Australian Government, including during the development of the Online Safety Industry Codes, as well as the Voluntary Online Dating Code, where Match Group played a leading role. In 2025, our first Transparency Report under the Code was published, reinforcing our commitment to accountability and continuous improvement (copy attached). Our second Transparency Report will be published in coming weeks.

At the state level, Match Group has engaged with the South Australian Government on proposed measures to restrict access to dating apps by individuals convicted of serious sexual and domestic

violence offences. This reflects our broader advocacy for solutions that strengthen preventative safeguards, including exploring appropriate access to offender information.

More broadly, Match Group collaborates with key agencies including the National Anti-Scam Centre, the Federal Attorney-General's Department and federal, state and territory law enforcement bodies. These partnerships support information sharing, improve responses to harm and help ensure our platforms continue to evolve to meet the expectations of regulators and the communities we serve.

5. Partnerships and Collaboration

Partnerships with NGOs are central to Match Group's trust and safety approach. Our business works with more than 100 organisations across over 20 countries to address critical safety issues both on and off our platforms. These partnerships help ensure our efforts are holistic, survivor-informed and reflective of the diverse communities we serve, spanning prevention, intervention and response.

At a global level, the [Match Group Advisory Council \(MGAC\)](#), established in 2018, brings together leading experts in areas such as gender-based violence, LGBTIQ+ inclusion, human trafficking and scam prevention. The Council plays an integral role in our safety-by-design approach, providing ongoing guidance to help ensure our platforms remain safe, inclusive and responsive to evolving risks.

In Australia, Match Group partners with organisations such as WESNET and Teach Us Consent to ensure our approach is locally informed and culturally relevant. Through these collaborations, users are provided with tailored education, resources and access to support services aligned with local needs.

Our NGO engagement focuses on both user education and expert advisory. Match Group collaborates with partners to equip users with practical safety knowledge on issues such as consent, healthy relationships, scam prevention and safer dating practices. At the same time, NGO partners provide critical input into our policies, product features and safety strategies, supporting a user-centred and trauma-informed approach.

There is regular engagement with NGO experts on emerging risks and trends, drawing on their expertise to inform how we design products, respond to incidents and communicate with users. These partnerships also contribute to research initiatives that shape our safety campaigns and long-term strategy. Match Group regularly convenes NGO roundtables and support partner-led events and survivor services globally to maintain these strong connections.

6. Access to Sex Offender Registers

Match Group's terms and community guidelines ban users who are convicted sex offenders. In the United States where Match Group brands have programmatic access to convicted sex offender registers, if a convicted offender is detected as being on one of our apps they are permanently removed from all our platforms.

In the past year Match has made representations to State and Territory Governments seeking programmatic access to sex offender registers to prevent known offenders from accessing our platforms and, as mentioned above, were instrumental in the South Australian Government's recent decision to bar domestic violence and sex offenders from online dating services for ten years following conviction.

Match Group believe the South Australian decision is a good step in prohibiting known offenders from accessing dating apps and have encouraged other jurisdictions to follow the South Australian lead. At the same time Match Group continues to push for access to offender registers as a further step in proactively improving dating app safety and would encourage the inclusion in the Action Plan of a recommendation that States and Territories give this proposal further consideration. Match Group acknowledges that the proposal raises privacy and data retention issues but believes these can be addressed while delivering improved safety outcomes.

7. Answers to Questions in the Consultation Paper Relating to Technology Facilitated Abuse and Online Platforms

1. What current or emerging issues should the Second Action Plan address, including in relation to coercive control and technology-facilitated abuse? (Page 45)

The Second Action Plan should treat technology-facilitated abuse as a pattern of conduct that can move across platforms, devices and into the physical world, rather than as a series of isolated online incidents. In online dating, technology-facilitated abuse can include persistent unwanted contact, impersonation, account compromise, location tracking, threats, image-based abuse, sexual extortion, financial abuse and the use of multiple or replacement accounts to evade a block or ban. Critically, these are cross-platform phenomena; we observe that perpetrators of harm rapidly move from dating services like ours (which are extensively and proactively moderated) to messaging or social media platforms which may have fewer safeguards.

A national response should therefore combine prevention, early intervention, enforcement and recovery. Priorities should include:

- nationally consistent definitions and measurement of technology-facilitated abuse, stalking and coercive control, focused on patterns, cumulative harm and repeat perpetration;
- safety-by-design expectations appropriate to the function and risk profile of each service, including proportionate identity and age assurance, proactive detection supported by human review, controls that give users greater agency, and continuous testing of safety interventions;
- accessible, trauma-informed reporting, including the ability to report after blocking or unmatching, preserve relevant evidence and receive clear information about outcomes and support services;
- lawful and appropriately safeguarded information-sharing and escalation pathways between platforms, police, eSafety and specialist services; and
- digital-safety capability across domestic, family and sexual violence services, police and courts, with particular attention to First Nations people, people with disabilities, LGBTIQ+ communities, migrant and refugee communities, and people in regional and remote areas.

Match Group's experience shows the value of layered safeguards: Face Check and other verification tools; harmful-message interventions; user filters and controls; in-app Safety Centres; Share My Date; trauma-informed reporting; and cross-brand action against users who breach safety rules.

Government action can complement these measures by establishing a legally authorised mechanism through which dating services can identify and exclude convicted sex offenders and serious domestic violence offenders who meet defined eligibility thresholds. This should include clear eligibility criteria, procedural fairness, data minimisation and security controls.

The Plan should also establish regular horizon-scanning with platforms, victim-survivors, specialist organisations and researchers so responses can adapt quickly as technologies and perpetrator tactics evolve.

2. How can governments, communities, schools, workplaces, online platforms and others better support people to recognise and respond to harmful attitudes and behaviours? (Page 46)

The Second Action Plan should build practical capability across the places where people live, learn, work and connect, using consistent language and clear actions: recognise warning signs; check in safely; interrupt or de-escalate where appropriate; document and report; and connect people with specialist support.

Respectful relationships and consent education should be sustained, not delivered as one-off sessions. It should cover digital consent, coercive control, sexual harassment, image-based abuse and sexual extortion, online misogyny, scams and the ways abuse can move from online contact to offline relationships.

Programs should be co-designed with users, victim-survivors and diverse communities, tested for unintended backlash, and reinforced by parents, sporting organisations, universities, workplaces and community leaders. Boys and men should be offered credible positive role models, emotional literacy and early, non-stigmatising pathways to seek help before harmful attitudes become abusive behaviour.

People are more likely to act when they know what to say, what not to do, how to preserve privacy and evidence, and where responsibility transfers to a specialist support service or police. Schools, workplaces and community services should provide practical, role-specific training, information and referral pathways. Responses should be trauma-informed and avoid victim-blaming, while maintaining clear accountability for people engaging in harmful behaviours.

Online platforms can support prevention at the point of interaction. Match Group's experience includes real-time prompts such as "Are You Sure?" and "Does This Bother You?", comment filters, verification tools, Safety Centres, safer-date sharing, and reporting processes that allow a user to report someone after unmatching. These measures create friction before a user creates or shared content which might be perceived as harmful, giving users greater control and making help-seeking easier, while avoiding overly paternalistic, top-down reactions which unduly restrict potentially legitimate expression. Platforms should also promote positive norms and local support resources in partnership with expert organisations. Match Group's work with WESNET, Teach Us Consent and the Match Group Advisory Council illustrates the value of combining product expertise with specialist and lived-experience advice.

Governments should coordinate common public messages, fund independent evaluation and encourage transparent reporting under frameworks such as the Australia Online Dating Code of Conduct. Success should be measured not only by campaign reach or reports received, but by improved recognition, safer interventions, reduced repeat harm and increased access to support. Education must complement - not replace - effective platform interventions, justice responses and adequately funded specialist services.

3. How should the Second Action Plan respond to current or emerging forms of harm affecting children and young people, including technology-facilitated abuse, harmful online content, and violence within peer and dating relationships? (Page 48)

The Second Action Plan should recognise children and young people as rights-holders and victim-survivors, while distinguishing children under 18 from young adults who are permitted to use our dating services. Dating platforms should prevent underage access through effective age assurance rather than self-declaration alone. Match Group combines age-gating, device and account signals,

automated image and text detection, human review, user reports and government-issued ID verification where necessary.

The Plan should address the way harms move between initial connection online and into offline relationships. Priorities include grooming and impersonation; cyberstalking and location tracking; image-based abuse, AI-generated sexual deepfakes and "nudification"; sexual extortion; pressure to share intimate material; exposure to misogynistic or violent sexual content; and coercive or violent behaviour in online interactions. Responses should therefore be coordinated across platforms, schools, services and law enforcement.

Key actions should include:

- sustained, age and developmentally appropriate education on respectful relationships and digital consent, beginning before harmful norms are entrenched and using realistic online and offline scenarios;
- youth-friendly, trauma-informed reporting and support across schools, health services, police, eSafety and digital platforms, with rapid evidence preservation, content removal and no victim-blaming;
- specialist responses for young people using violence or harmful sexual behaviours that prioritise safety, accountability and behavioural change without automatically criminalising trauma-related behaviour;
- co-design with diverse young people, including First Nations, LGBTIQ+, young people with disability, migrant and refugee communities, and regional and remote young people; and
- national research and outcome measurement tracking emerging technologies, repeat harm and abuse that moves between services.

For young adults using Match Group services, safety-by-design measures can reinforce this framework. These include verification, harmful-message prompts, user controls, localised Safety Centres and Healthy Dating Guides, safer-date sharing, reporting after unmatching, cross-brand enforcement and law enforcement cooperation.

No platform or age-gating solution can address these harms alone, and these efforts benefit from joint initiatives that amplify messaging through multiple channels and with multiple credible voices. Governments, families, schools, communities, specialist services and technology companies should share responsibility for equipping young people to recognise abuse, seek help early and help design the responses intended to protect them.

8. Conclusion

Match Group is committed to fostering safe, respectful and inclusive environments for all users, and we recognise the important role digital platforms can play in both preventing harm and supporting users.

As outlined in this submission, Match takes a proactive, safety-by-design approach, combining strong policies, product innovation, user education and collaboration with governments, law enforcement and NGOs, to help reduce risk and respond effectively to harmful behaviour. We believe continued partnership between industry, policymakers and community organisations is essential to address the complex and evolving nature of online-enabled harm, including through our proposal to access offender registers to prevent known offenders from accessing our platforms.