Dating Services Framework for User Safety

The ODA Model Code of User Conduct sets out who is expected by way of user conduct and behaviours. Users and others will reasonably expect there is an appropriate parallel Framework setting out what we think to be good practice on the part of service operators when it comes to their roles in making dating services as safe as possible.

The Framework sets out those core activities thought to be key to achieving this goal. The Framework is based on provisions originally set out in the ODA standard and guidance on "Online Safety and Protection" and dialogue with service providers, law enforcement and other stakeholders.

The Framework identifies issues thought to be central to user safety. It is guidance: a template services can choose when it is reviewing their policies and processes. Accordingly, the Framework is neither prescriptive nor mandatory. In bringing forward the Framework the ODA is not acting as an approvals or compliance body, but as a body seeking to ensure safety is at the heart of dating services.

The Framework reflects the core Principles of the Online Dating Association. Members of the ODA display the Association logo online to show this commitment to these Principles.

User advice and guidance

Service providers should give creative thought to when and how information can be given in ways that maximise user-awareness. Service providers have various opportunities to guide users on how to make best but also safe use of services. These include:

- at the point of sign-up
- when potential matches are presented
- when a user takes a subscription
- when users are alerted to interest from others through the messaging system

Advice and Guidance should at minimum address the risk of forms of online fraud and the risks to personal safety when meeting someone in person, particularly for the first time.

Services should highlight those behaviours and requests that might signify a scammer. Services that provide more secure in-service communications platforms should point out the benefits of these and risks of being taken off-site.

Service providers should look to make use of advice and guidance on safety online that may be produced by other agencies seeking to prevent fraud or other forms of harm such as stalking, harassment and revenge porn.

Addressing user safety

Services should give users a good understanding of what is and is not done in relation to safety and should be clear on where and why responsibility for certain risks must lie with Users.

Services should explain the steps the service can take to moderate users, making clear and also making clear the limits to what is permissible vis criminal record or other checks and, therefore, that they cannot guarantee the accuracy of profile information. Services should highlight ways in which users can take steps to check another user's profile; being clear where these may be helpful but not 100% assured.

As part of best practice, services are expected to:

- Make Users aware of what constitutes unacceptable and illegal behaviour while using a dating service. The Model Code of User Conduct might help services in reviewing the content of any statement of their expectations. Services should give thought to how these expectations are shared with users in a way that ensures they are seen and understood, for example at point of registration.

- Ensure that Users are able easily to report any abuse/harm to the dating service and encourage Users to do so. Services may then need to consider whether their customer support set-up is able to address potentially sensitive issues as well as routine contractual and operational questions, and if not signpost to specialist support services.

- Ensure that all reports are responded to quickly and appropriately allowing action to highlight and secure a change in behaviour where possible and enable service providers to remove a profile and terminate an individual's use of the service where that is an appropriate response.

- Have arrangements in place for dealing generally with reports within a set timeframe and addressing when and how actions taken may be explained to the person who reported the incident. Thought should be given to whether it is possible to alert others at possible risk whilst safeguarding the person making the report.

- Actively moderate user profiles, ensuring that appropriate arrangements exist to detect fraudulent or misleading profiles and inappropriate or harmful content and behaviours, and to remove such profiles from the service as soon as possible.

- Be alert to the possibility of under 18s trying to join a site. Services should be clear on the age restrictions that apply. In addition to profile picture and content checks, services should consider forms of cross-checking with other digital platforms and should actively encourage users to report any possible under-age individuals on the service.

- Respond fast to any reports of an under-age person that has managed to get onto the service, removing the profile and considering whether there is other action necessary specific to the individual incident.

- Be alert to any report suggesting another user is behaving in ways that are a cause for concern, distress or actual harm. Services should have the ability to remove such users. If serious issues arise operators should not hesitate to encourage a user to report the matter to their local police force, anonymously or otherwise.

- Investigate whether an individual or profile removed for serious unacceptable behaviour has been in contact with others on the service and might pose some threat to the safety of these other users.

- Consider whether it is appropriate to refer a user with concerns to law enforcement agencies or charitable bodies or others that specialise in safeguarding, protection and victim support.

- Understand the legal basis on which law enforcement or other regulatory agencies may require information and co-operate with these agencies.

Managing the risk of fraud

Services should not themselves create fake profiles to seem to populate a service or knowingly allow users or any other party to create and post fake profiles to attempt a fraud.

Services should use best endeavours to identify and remove scammer profiles, using software analytics, any data feeds from law enforcement bodies, agencies with sector-specific expertise and technology alongside profile monitoring and user reporting tools.

Services should allow users to report others if they suspect fraud or believe the person in question is a risk to the safety of others. Services should monitor these report channels and be ready to act promptly to remove wrongdoers. Where possible Services should give feedback on this to those making reports.

Where there is clear and demonstrable evidence of actual or attempted fraud, Services could look at whether that user has had significant and close contact with people other than any known victim, giving thought to whether it is possible to alert others at possible risk whilst safeguarding the person making the report.

Services should always advise a victim of a scam to inform law enforcement agencies to help with investigation or prosecution and allow expert victim support officers to act to prevent further harm.