Online Dating & Discovery Association

To: Ofcom (via online form)

1st December 2025

RE: CALL FOR EVIDENCE: STATUTORY REPORTS FOR AGE ASSURANCE AND APP STORES

The Online Dating and Discovery Association (ODDA) is the recognised trade body for the sector with a mission to create safe, responsible and enjoyable experiences for everyone. Representing nearly 500 brands worldwide, the ODDA and its members are committed to keeping children off services designed for over-18s and welcomes the opportunity to respond to this important call for evidence.

How have regulated service providers used age assurance for the purpose of compliance with the duties set out in the Act?

While we recognise that the number of children attempting to access online dating and social discovery services is low, our sector has widely welcomed the introduction of the Online Safety Act (OSA).

As a key component of the OSA, the adoption of age assurance technology across our sector is gaining momentum. Since the Children's Codes came into effect during the summer, our members are using a variety of age assurance methods that are capable of being highly effective. These include photo-ID matching, facial age estimation, mobile network operator checks, credit card checks and email-based age estimation. Some are using more than one to prevent under-18s accessing their services. We are also aware that while most of our members have turned to third-party providers for age assurance solutions, some have developed their own.

In terms of where age assurance is being used, we have seen a mix across the sector with some using it during the onboarding process, while others where age-gating is required (for example, at the point where content for over-18s becomes accessible). As age assurance becomes more commonplace, we expect our members to review and refine their approaches to continually improve its accuracy, reliability and fairness.

How effective has the use of age assurance been for the purpose of compliance with the duties set out in the Act?

It is difficult to provide a comprehensive answer at this stage considering the relative newness of the duties coming into effect, but in speaking to our members, the response so far has been mixed as we explain below.

Has user privacy, cost, or any other factor prevented or hindered the effective use of age assurance, or a particular kind of age assurance, for that purpose?

Our members have identified a number of factors that have either prevented or hindered the effective use of age assurance. These include:

Friction:
Online platforms work hard to develop customer journeys that require as little friction as possible while keeping their users safe from harm. Implementing age assurance technology creates additional friction that increases drop-off rates. One of our members for example, a small, UK-based dating platform, has witnessed a significant in-crease in drop-off rates for users under the age of 25. The need for additional measures to verify the identity of these individuals has resulted in them exiting the 18-25 market completely.

Data Privacy and Security:
Recent high-profile data breaches and Government messaging around the risks of sharing personal information, have understandably led to users being concerned about data privacy and security. We have heard anecdotally that drop-off rates on smaller, less well-known services are higher than they are on larger, more well-known services because users are less confident about sharing personal information with a service they may not be familiar with.

Cost:
Carrying out age assurance checks creates an additional cost that cannot always be easily absorbed or passed on to the customer. This is particularly problematic for smaller platforms who may have to delay investment, recruitment or product innovation. However, we recognise that the average cost of age assurance checks has fallen considerably in the past 12 months as new technologies emerge. Despite this, cost continues to be a significant barrier to implementation.

Online Crime:
We have started to see emerging evidence of fraudsters using the requirement to implement age assurance technology as an opportunity to target users by creating fake adverts that mimic legitimate age assurance providers. We are concerned that this will further compound concerns around data privacy and security, resulting in even higher drop-off rates. In fact, we wrote to Ofcom CEO Melanie Dawes earlier this year on this exact point following evidence provided to us by one of our Associate Members.

Interoperability:
Users of online dating and social discovery services typically sign-up to more than one service. This means that they are potentially required to verify their age on every service they sign up to.

To address these issues and improve the effectiveness of age assurance, we encourage Ofcom to use this call for evidence to re-consider its approach and encourage greater flexibility in the way in-scope service providers implement age assurance solutions.

We also think that transferable tokens should become a minimum standard for all providers so that when a user verifies their age on one service, that token is stored on their device and can be used for verifying their age on other services. This measure would alleviate the concern around friction.

We think there is also an opportunity for Government to explore the possibility of including age assurance in its proposals for Digital ID.

What role do app stores play in children encountering:

a) user-to-user content that is harmful to children;
b) search content that is harmful to children; or
c) regulated pornographic content

The ODDA and its members have long argued that App stores have an incredibly important role to play in preventing children from accessing age-inappropriate con-tent. This also includes individual apps listed in the store.

In our view, mobile phone users are already familiar with App store age checks when setting up their account as without it, they are unable to access any age-restricted content. This data is kept by the App stores and could easily be used to verify the users age at zero cost and zero friction.

However, we recognise that this doesn't solve the issue of in-scope services who operate outside of the mobile eco-system. To address this, we encourage Ofcom to look beyond App Stores and consider other centralised services which provide the same benefits, e.g. devices, internet service providers, and the government themselves with the forthcoming Digital ID.

Do you think that children's online safety would be better protected from the content types listed in Section B, Question 1 by:

a) greater use of age assurance;
b) particular kinds of age assurance; or
c) other measures, at the app store level?

The ODDA believes that greater use of age assurance at App store level would better protect children from the content types listed in Section B and is something our members would strongly support for the reasons set out above. We also think that setting and enforcing terms of service at App Store level to prevent under-18s accessing inappropriate content would be a welcome move.

While we do not have a strong view on the kinds of age assurance that should be used, we recognise that there are already many solutions in the market that are capable of being highly effective and that the industry is evolving rapidly. We think this creates an exciting opportunity that would help address concerns around friction, cost and data privacy/security.

We also do not see any barriers or risks to implementation. However, we think a wider consultation with in-scope services is required to ensure that any unintended consequences are fully understood.

Yours sincerely,

Simon Newman

Simon Newman
Chief Executive Officer

simon@theodda.org