2025

illuminate
tech.

Online Dating &
Discovery Association

The UK Online Safety Act: **A Roadmap for Dating Services**

Foreword

The Online Safety Act is a ground-breaking piece of legislation that introduces a number of new duties for online services. As the global voice for the online dating and social discovery sector, the ODDA is committed to helping our members understand what they need to do in order to comply with these new duties.

We're therefore delighted to have collaborated with **Illuminate Tech** on this report which clearly sets out how it applies to our sector and the actions our members need to take to ensure compliance.

Simon Newman

Simon Newman
Chief Executive Officer

Online Dating &
Discovery Association

Preface

This report is designed to help dating services understand what is expected of them under the UK Online Safety Act (“the OSA”; “the Act”). **Delivered in collaboration with the Online Dating & Discovery Association (ODDA), it sets out**

- how dating services are captured by the Act,
- information on the regulator and its enforcement powers,
- the key steps to compliance.

As a regulated service, dating services must conduct risk assessments and keep up-to-date written records. They must then implement measures to mitigate the risk of harm, and continuously review the effectiveness of these measures.

This report applies the obligations of the OSA to ODDA members’ specific context. This report is not designed to give tailored advice, but instead empowers dating service providers to take charge of their approach to online safety compliance.

For more information, reach out to hello@illuminate.co.uk.

Meet the co-founders

George Billinge

CEO

George is an online safety policy specialist with expertise helping tech companies navigate shifting regulatory requirements. While leading the delivery of tech-literate policy in Ofcom's online safety team, he worked to foster alignment between regulators, particularly on age assurance. He has advised businesses on compliance strategies and contributed to research and development projects funded by the Australian Government, Innovate UK, and the European Commission. His work bridges the gap between policy and product teams, enabling companies to leverage transparency to build trust with their users.

✉ **george@illuminatetech.co.uk**

Asad Ali, PhD

CTO

Asad is a leading expert in digital identity and age assurance technologies. Before joining Illuminate Tech, he led Ofcom's Digital Identity team, overseeing research programs to inform the Online Safety Act. With a PhD in Digital Identity, he began his career lecturing at King's College London, before supporting companies transform their approach to identity and access management. He specialises in building bespoke approaches to evaluating the effectiveness of online safety tech.

✉ **asad@illuminatetech.co.uk**

Table of Contents

Part 1: The Online Safety Act

The UK Online Safety Act (commonly referred to as the "Act" or the OSA) establishes one of the most comprehensive online safety regulatory frameworks in the world. Enacted into law in October 2023, the Act introduces a long list of new duties on providers of dating services. These duties include conducting sufficient risk assessments and implementing "proportionate systems and processes" to mitigate the risk of harms, with a focus on illegal harms and content that is harmful to children.

Fundamentally, the OSA places a duty of care on providers of online services towards their users.

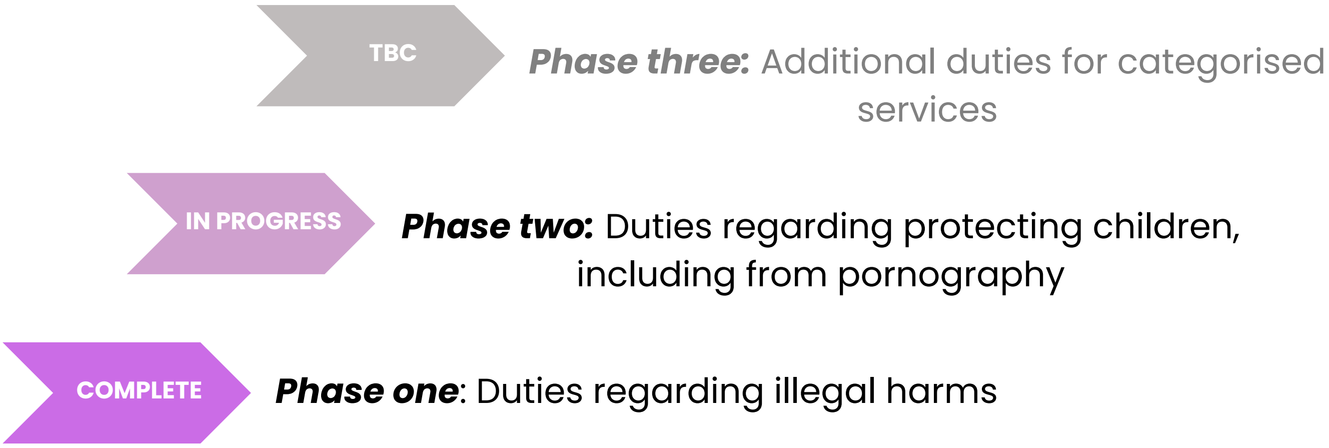
Step-by-step, dating services must:

1. **Conduct a sufficient risk assessment**
2. **Identify appropriate measures**
3. **Implement these measures effectively**
4. **Monitor the effectiveness of chosen measures**

All of the steps must be captured in the form of a **written record.**

Importantly, the Act is not prescriptive—it is up to companies to decide what safety measures would be appropriate given the risks posed by their functionalities.

The Act utilises a risk-based approach to understanding threats to users. Underpinning the entire Act is a focus on reducing the risk of harm to children. There are three roll-out phases:



TBC

Phase three: Additional duties for categorised services

IN PROGRESS

Phase two: Duties regarding protecting children, including from pornography

COMPLETE

Phase one: Duties regarding illegal harms

1.1 The regulatory body and its enforcement powers

The regulatory body is the UK Office of Communications, known as Ofcom. Besides being responsible for ensuring online services meet their obligations under the OSA, they oversee telecommunications, TV, radio, and the postal service.

The Act has given Ofcom significant enforcement powers to enforce the UK's new online safety regime, including the ability to impose fines up to

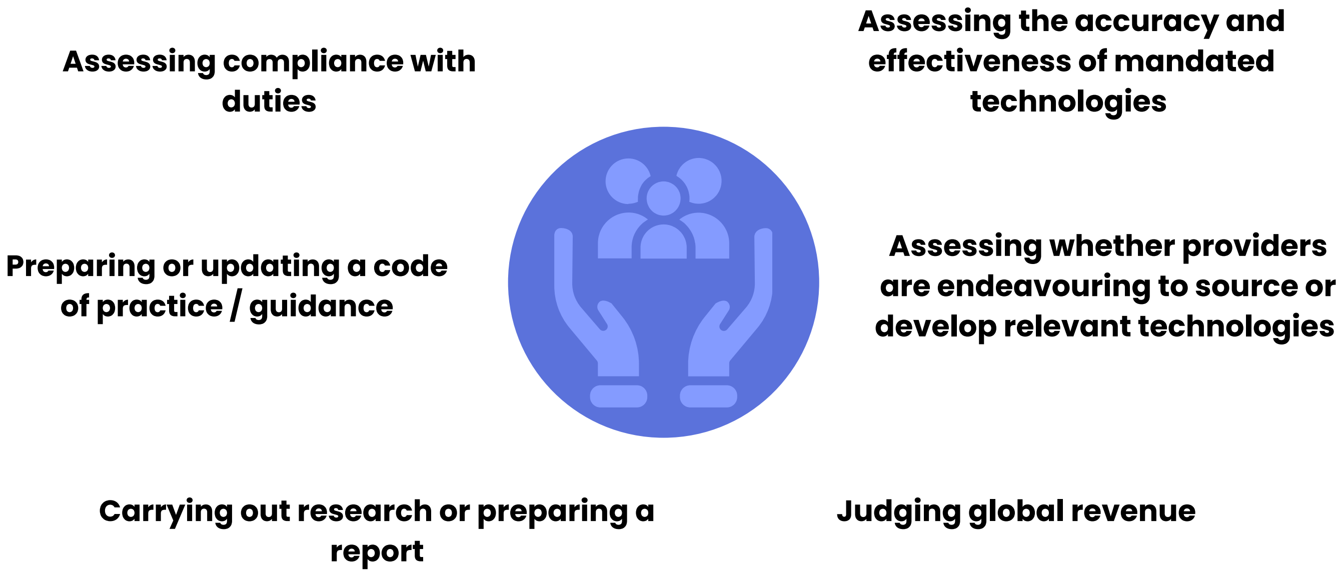
£18 million or 10% of a platform's global turnover (whichever is greater).

Ofcom can also impose business disruption measures and in the most serious cases, criminal penalties for senior managers [1].

An example of a business disruption measure is a **service restriction order,** in which Ofcom can impose restrictions on services that dating apps rely on to generate revenue. These ‘ancillary services’ include payment processing services, identity verification tools, location services, and ad servers [2]. In other words, **Ofcom has the authority to negatively impact your business through the suspension of third-party tools which facilitate your revenue-generating activities.**

OFCOM’S INFORMATION GATHERING POWERS

Another important feature of Ofcom’s powers is its ability to request information from regulated services or providers of ancillary services for purposes such as below.



Assessing compliance with duties

Assessing the accuracy and effectiveness of mandated technologies

Preparing or updating a code of practice / guidance

Assessing whether providers are endeavouring to source or develop relevant technologies

Carrying out research or preparing a report

Judging global revenue

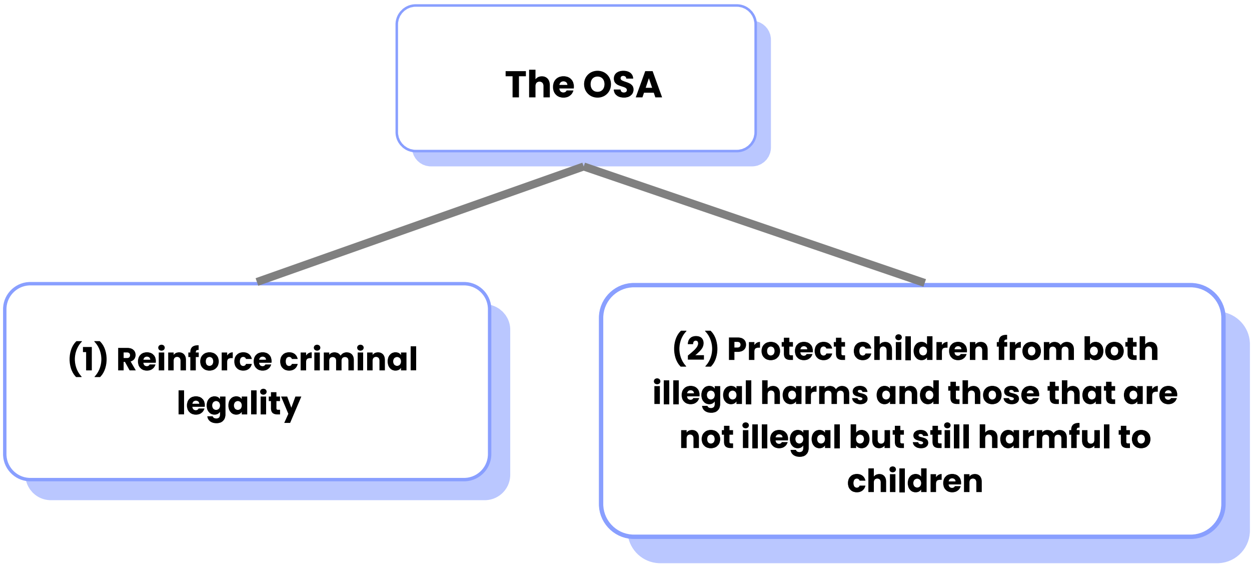
Figure 1 Ofcom can requestion information for various purposes (OSA, Part 7, Section 6).

[1] See Ofcom’s Online Safety Enforcement Guidance for more details
[2] For further examples. see 144(12) of the OSA.

1.2 What the Act sets out to do

It might be simpler to start with what the Act does *not* do. The Act does not instruct Ofcom to remove pieces of content or take down specific accounts, nor to investigate individual complaints. Instead, **the goal is to tackle the root causes of online content that is illegal and/or is harmful to children.**

The Act can be broadly understood to do two things:



The OSA

(1) Reinforce criminal legality

(2) Protect children from both illegal harms and those that are not illegal but still harmful to children

(1) points to the main prerogative of limiting harms by focusing on illegal content outlined in UK criminal law. Dating services must assess the risk of harm arising from illegal content in-scope of UK criminal law. The Act groups 130 offences into 17 types of priority 'illegal content,' along with 8 more types of non-priority illegal content [3].

However, the Act is not completely confined to the limitations of existing law. To keep up with the different ways harms manifest online, the Act introduces provisions to existing laws to include (non-priority) illegal content like cyberflashing and epilepsy trolling.

[3] View the Risk Assessment Guidance for the list of priority illegal content.

(2) points to the emphasis on protecting children from harm. There are additional requirements for regulated services to assess the risk of harm they pose to children, and subsequently the measures they adopt to mitigate those risks [4].

1.3 How the Act captures dating services

With over 100,000 services in scope, the Act covers platforms that have a significant number of UK users, or those which have the UK as one of their target markets [5]. The Act applies to:

User-to-user (U2U) services –i.e., social media, dating services, messaging services, marketplaces, cam sites, fan sites, tube sites, and video-sharing services.

Search services –i.e., search engines.

Pornography publishers –i.e., pay sites and studios.

Part 3 includes U2U and search services while **Part 5** includes platforms dedicated to publishing non-user-generated porn. At first glance, it seems only **Part 5** services contain pornography, but this is not true. For example, tube sites (e.g., PornHub) host user-generated and hence are captured within **Part 3**. Reddit is a U2U service which hosts adult content. Dating platforms which allow image-sharing carry the risk of user-generated porn, and the same risk applies to most social media platforms.

[4] See Section 2.1 for a visual overview of all the requirements for regulated services.
[5] 'Significant number' is not defined in the Act. Services must explain their judgment if they think they do not have a significant number of UK users.

Ultimately, Ofcom adopts a holistic view: factors such as the platform's business model, existing safety features, and how it presents itself in the market all impact how each risk should be assessed.

WHY ARE DATING APPS 18+ ?

Not many dating services would refute the idea that the hunt for romance and/or intimacy in the digital space increases the likelihood of exposure to sexual material. Even fewer would disagree with taking steps to prevent children from interacting with adults in such contexts. Such reasoning explains why virtually all dating services already include an 18+ condition in their Terms of Service. **Risk-based thinking isn't new to most ODDA members.**

Historically, there has been a gap between the existence of an 18+ user condition and the steps services have taken to enforce it. Evidently, there is a clear distinction between pornography services and dating apps. However, certain dating apps allow for explicit (legal) image-sharing. Under the Act, pornography is defined as content produced for the purpose of sexual arousal [6]. By this definition, **dating apps can and do allow for user-generated pornography.**

Beyond the risk of sharing intimate images, dating apps match random users in romantic or sexual contexts, meaning adult-child interactions should be minimised as much as possible to mitigate the risk of illegal harms like grooming and CSAM.

With the introduction of the Act, dating services must now pay close attention to the risk of children accessing their platforms; CSEA is a priority illegal harm. Pornography is not illegal, but the Act does deem it harmful to children [7]. **There is now a legal obligation to put in effective measures to enforce safety policies like the 18+ condition in order to mitigate the risk of illegal harms.**

[6] See Section 236(1) of the Act.
[7] Keep in mind that 'extreme pornography' is illegal, and it also is a risk where image-sharing exists.

WHAT THE ACT CHANGES FOR DATING SERVICES

Dating apps are used to thinking about risks and how to mitigate them. What the Act does is raise the bar, requiring services to structure their thinking—through the formulation of various written records— on how to protect their users. Based on these written records (e.g. the illegal content risk assessment), dating services have a legal duty to implement proportionate measures and keep tabs on their effectiveness.

A result of the Act "raising the bar" is the introduction of age assurance, defined as the process used to determine whether a user is a child or an adult. In short, age assurance is directly mandated for **Part 5** services because they publish adult content, and age assurance is indirectly mandated for **certain U2U services** because they have the risk of exposing adult content to children. The table below compares possible paths to age assurance:

Service type	Illegal content risk assessment	Children's access assessment	Children's risk assessment	Age assurance
Dating apps	✓	✓	✓	✓
Tube sites; cam sites; fan sites	✓	✓	✓	✓
Part 5 services	✗	✗	✗	✓

Table 1 How dating services land at age assurance compared to other services.

The Act takes into account context when regulating services—how high of a risk something is, what a service claims in its policies, and the effectiveness of its measures behind these claims. That is why dating services are not mandated to adopt age assurance before going through all the required steps (See Part 2).

AGE ASSURANCE AS A PROCESS

There are a wide range of age assurance solutions on the market, and picking the right product for your service is an important part of complying with the Act. Age assurance is often perceived as a strict "age gate" that risks introducing a significant amount of friction into the user journey. However, the Act encourages regulated services to think of age assurance as a holistic process; a number of steps that can be taken to prevent children from accessing services on which they are exposed to a high risk of harm.

Regardless of the approach to age assurance a dating service chooses, it is vital to keep a clear written record outlining

i) why you have decided on a particular approach,

ii) how it is effective at mitigating the risk of children accessing online spaces designed for adults.

The OSA requires service providers to record their thought processes in a clear, truthful manner. For example, dating services must ask themselves why they include an 18+ condition. Then, they must ask themselves how they effectively enforce that condition.

WHY OFCOM FINED TIKTOK £1.875 MILLION IN 2024

TikTok was fined £1.875 million by Ofcom for failing to accurately respond to a formal request for information about its parental controls safety feature [10]. Ofcom issued the request to assess the tool's effectiveness in protecting teenage users. Statutory information requests like these are expected to frequent services who adopt child safety features or proclaim to be 18+, as these aim to protect children from harm—a clear focus for Ofcom and the OSA.

How you report on the efficacy of a measure matters.

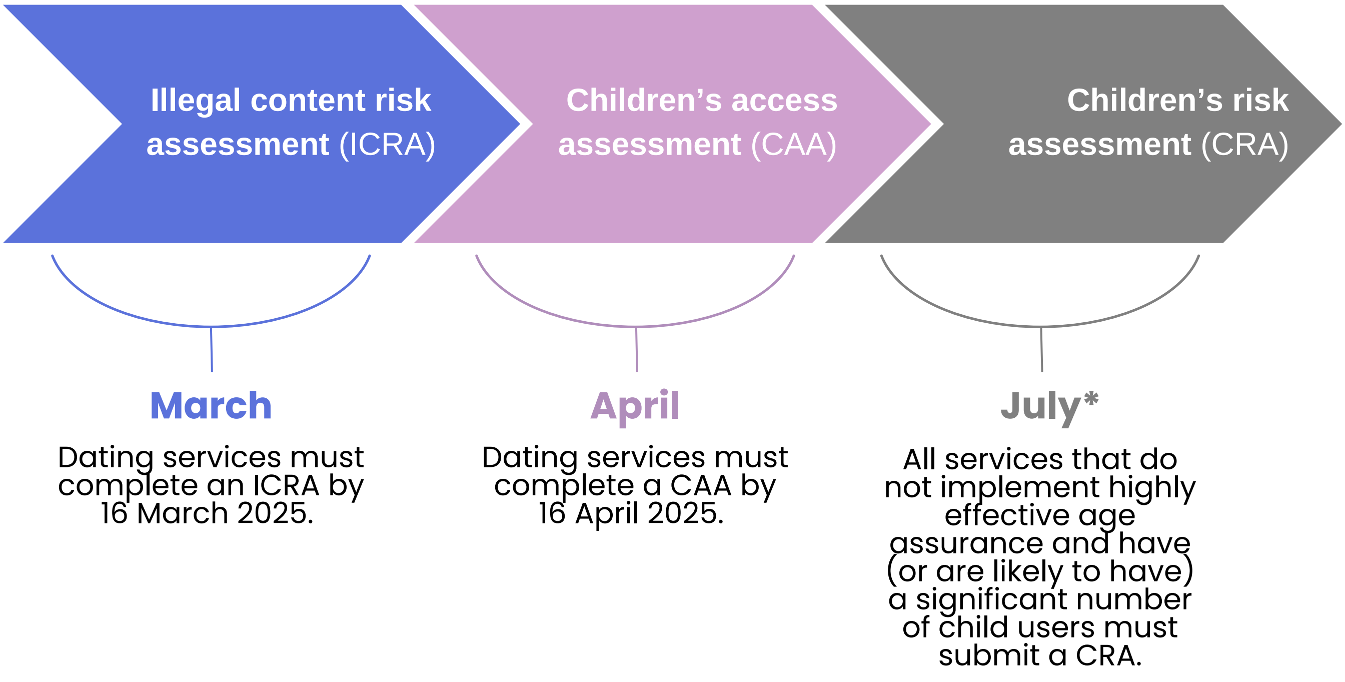
Egregious harms such as CSAM and grooming can occur when platforms do not effectively manage their 18+ promise or safety features. Services should prioritise measures they feel can withstand the regulator's scrutiny and report truthfully to minimise the risk of fines.

Part 2 will explain how Ofcom prioritises harmful content into a set of requirements for dating services.

[10] See more information here.

Part 2: Compliance for dating services

Part 1 of this report described the risk-based approach to tackling harm set out in the Online Safety Act. Now, **Part 2** will highlight actions dating services need to take in the upcoming months, and describe key milestones to look out for from Ofcom. **Part 2** also provides a case study on the relationship between functionalities, the risk of illegal harms, and measures by focusing on a widespread dating platform functionality—matching algorithms.



Illegal content risk assessment (ICRA)
Children's access assessment (CAA)
Children's risk assessment (CRA)
March
April
July*

Dating services must complete an ICRA by 16 March 2025.

Dating services must complete a CAA by 16 April 2025.

All services that do not implement highly effective age assurance and have (or are likely to have) a significant number of child users must submit a CRA.

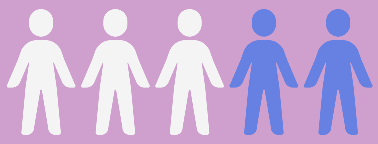
*Dependent on when in Spring 2025 Ofcom releases its CRA guidance

Figure 2 Compliance deadlines for the OSA

2.1 4-steps to the illegal content risk assessment

Ofcom published their guidance to the **illegal content risk assessment (ICRA)** in December 2024, stating all regulated services must complete the ICRA within 3 months of the guidance being published. To meet the requirements of the ICRA, **services should assess the risk of harm arising from each of the 17 kinds of priority illegal content, and other non-priority illegal content** [11]. Cyberflashing is an example of non-priority content that should be included in a dating service's assessment but will probably be negligible in, for example, online chess platforms.

Romance fraud is up 60% since 2019 [12]. Fraud is a priority illegal harm.



2 in 5 people are asked for money while looking for love online [13].

Ofcom has published evidence-based guidance on online harms, the risks associated with service characteristics, and a risk assessment template. Although the Act is not prescriptive, the guidance sets out an approach which services can take to achieve compliance. We have summarised the four steps on the next page.

[11] See the complete list of illegal content in Ofcom's Register of Risks
[12] Read the BBC article here.
[13] According to UK Finance.

STEP 1 – UNDERSTAND THE HARMS

- **Identify the 17 kinds of priority illegal content.**
- **Identify all kinds of CSEA** (Grooming and CSAM) that can manifest on your service.
- **Identify whether there is a risk of other illegal content** (non-priority offences). These include cyberflashing and encouraging/assisting in self-harm.

STEP 2 – ASSESS THE RISK OF HARM

- **Consider the characteristics of your service.** These include its user base, functionalities, algorithms, and the business model.
- **Find the Risk Profiles** in the Register of Risks. Risk Profiles link risk factors (i.e. platform features and functionalities) to one or more kinds of illegal harm.
- **Use your judgement to assign a risk level of high/medium/low or negligible** to each of the 17 kinds of priority illegal content and to the other illegal content you have chosen to assess.
- **Assess the risk of your service being used for the facilitation or commission** for each of the 17 kinds of priority illegal content.
- **Ensure you record your evidence/reasoning** for each risk assessment.

STEP 3 – DECIDE MEASURES, IMPLEMENT, & RECORD [12]

- **Decide what measures you need to take to reduce the risk of harm.** This is your plan for risk mitigation.
- **Implement all measures to start managing risk.**
- **Re-evaluate when there's a change.** Service providers are held responsible for any changes to existing systems, processes or other measures as these could affect your risk levels.
- **Record the outcomes of the risk assessment**.

STEP 4 – REPORT, REVIEW & UPDATE

- **Report on the risk assessment and measures** via relevant governance and accountability channels. These channels must exist within your organisation.
- **Monitor the efficacy of your safety measures.**
- **Review your risk assessment** every 12 months, or if Ofcom makes a significant change to a Risk Profile.

Deadline for the ICRA:
16 March 2025

2.2 Children’s access assessment

All services must carry out a children’s access assessment (CAA) by mid-April 2025 to determine whether children are able to, or are likely to, access the service [13]. Services must first check if it is *possible* for a child to normally access the service. If the answer is yes, the service moves on to assess if it is likely for a significant number of children to be users of the service.

The only way a service can state that children cannot normally access their service is by implementing ‘highly effective age assurance’ (HEAA). If a service chooses to implement HEAA, they should keep a written record of how they have assessed the age assurance against each of Ofcom’s four criteria (see next section).

WHAT IS ‘HIGHLY EFFECTIVE’ AGE ASSURANCE?

Ofcom takes a principles-based approach to defining highly effective age assurance: it should be **technically accurate**, **robust**, **reliable**, and **fair**. The identity & age verification industry is advancing rapidly, but not all age assurance solutions on the market are created equal. Ofcom is aware of this and does not want to stifle innovation. However, it does suggest methods capable of being highly effective:

[12] Use the Illegal Content Codes of Practice to find recommended measures. Note: you are allowed to seek alternative measures outside of the Codes.
[13] Children refers to anyone under 18.

Methods capable of being highly effective
Open banking
Photo-identification (photo-ID) matching
Facial age estimation
Mobile-network operator (MNO) age checks
Credit card checks
Email-based age estimation

Methods not capable of being highly effective
Self-declaration of age
General contractual restrictions on the use of the service by children

! **IMPORTANT:** Integrating a particular method of age assurance is not enough to guarantee compliance. What matters is how you implement it in a way that meets Ofcom's criteria.

For example, service providers must record how technically accurate the chosen method is by ensuring there are available metrics to back up its performance.

Table 2 Age assurance types capable of being highly effective (Ofcom 2025).

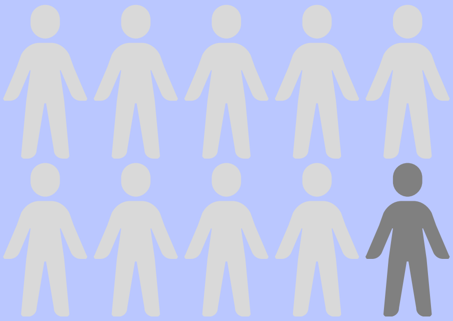
It is crucial to record how you have assessed age assurance against Ofcom's criteria**. If you implement age assurance in a way that demonstrates the four criteria, you do not need to complete a children's risk assessment (CRA)** [14].

2.3 From risks to measures

We expect that dating services will implement highly effective age assurance (HEAA), as it is the easiest way to enforce their 18+ user condition and the only way to avoid conducting a children's risk assessment. This does not mean such services are exempt from implementing measures against CSEA content (i.e., grooming and CSAM) or illegal harms in general.

[14] The exact deadline for the CRA will realise once Ofcom publishes its final guidance, expected in Spring 2025.

HEAA is a strong measure against grooming but is not a comprehensive measure against CSEA—CSAM can still manifest in services that have a very low risk of child users.



Dating services can be exploited to solicit CSAM. In a study of 10,000 people, **1 in 10 reported being approached to exploit their own children or children they have access to.**

Figure 2 Study by Teunissen, C., Boxall, H., Napier, S. & Brown, R. (2022). The sexual exploitation of Australian children on dating apps and websites.

Evidence from studies like the above underscore Ofcom's requirement for dating services to **assess the risk of their service being used for the commission or facilitation of each kind of priority illegal content.**

NO BLANKET MEASURES

Each dating service has its own specific functionalities and characteristics which result in varying risks, making it impossible to recommend a list of 'blanket' measures. Moreover, the Act endorses the principle of "proportionality" when it comes to implementing measures [15]; smaller platforms that rely on community-based content moderation are not expected to implement the same measures that may apply to bigger platforms.

However, multi-risk services—i.e., services at medium or high risk of two or more kinds of illegal harm—are expected to implement more extensive and effective measures. The specific measures depend on the nature of the risks identified in the ICRA and can possibly include proactive technologies like hash-matching. Therefore,

[15] See 10(2) of the Act.

a service's risk assessment dictates what sort of actions Ofcom will expect it to take in order to mitigate against online harms.

LOOKING AT MATCHING ALGORITHMS AS A RISKY FUNCTIONALITY

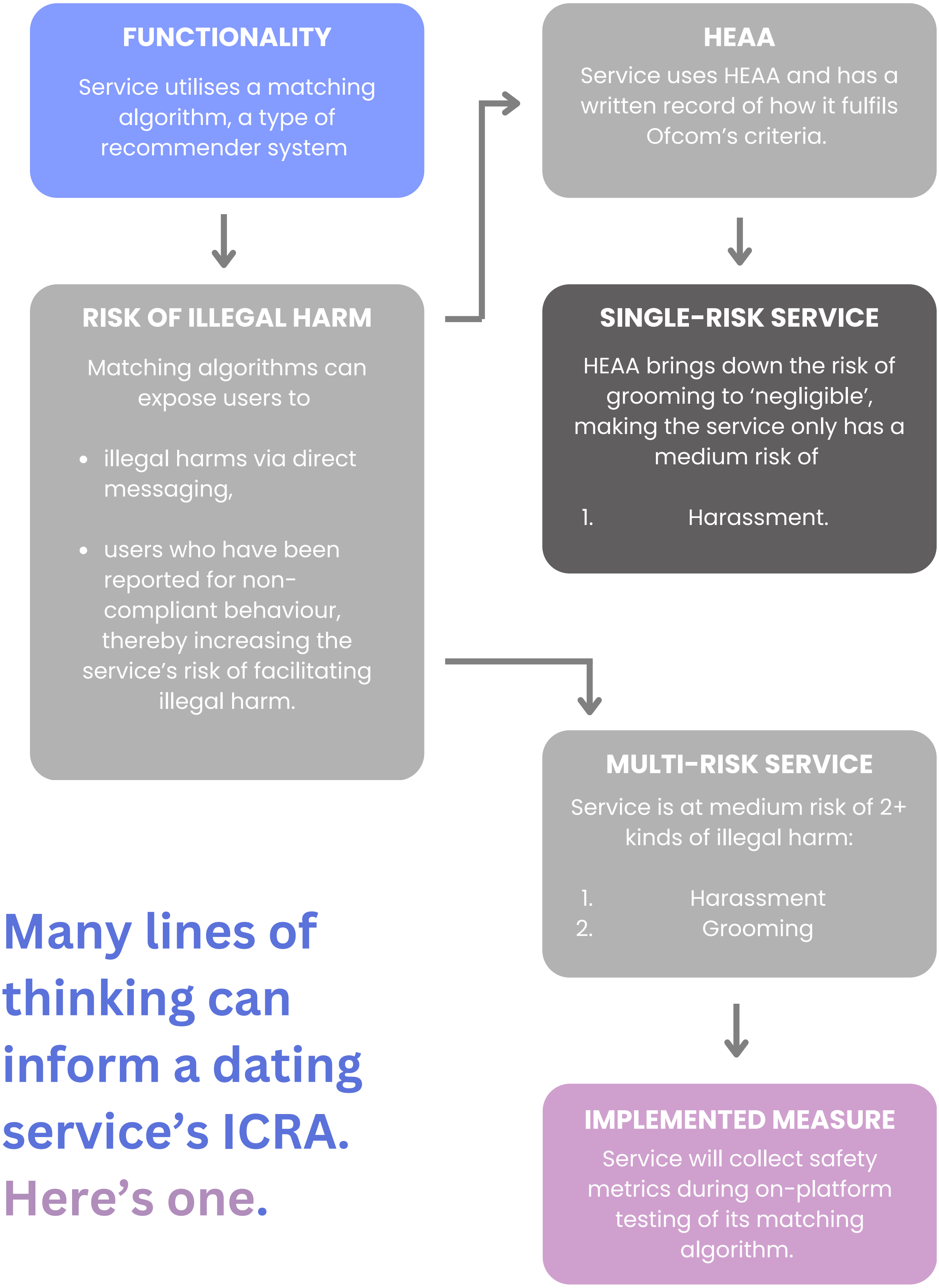
Matching algorithms (a type of recommender system) are an integral aspect of many dating services. They determine how users are recommended to each other based on criteria such as preferences, behaviour, location, and social media data.

Different services use different algorithms, but most services conduct on-platform testing in order to improve match quality. **If you are a multi-risk service that conducts on-platform testing of your matching algorithm, Ofcom recommends you collect safety metrics during on-platform testing of your matching algorithm** [16].

Figure 3 is an example of the many lines of thinking that can inform a dating service's ICRA. It's important to note that the risk of harm can arise from a combination of service characteristics, rather than just one characteristic (functionality or otherwise) in isolation. **The example below highlights the compounding effect on risk** from the matching algorithm, direct messaging, and the lack of an effective way of ensuring reported users are hidden from the view of those that reported them [17].

[16] See Chapter 7 in Volume 2: Service design and user choice for more details

[17] Hinge has an example of an effective reporting feature. View their reporting policy..



FUNCTIONALITY

Service utilises a matching algorithm, a type of recommender system

RISK OF ILLEGAL HARM

Matching algorithms can expose users to

- illegal harms via direct messaging,
- users who have been reported for non-compliant behaviour, thereby increasing the service's risk of facilitating illegal harm.

HEAA

Service uses HEAA and has a written record of how it fulfils Ofcom's criteria.

SINGLE-RISK SERVICE

HEAA brings down the risk of grooming to 'negligible', making the service only has a medium risk of

1. Harassment.

MULTI-RISK SERVICE

Service is at medium risk of 2+ kinds of illegal harm:

1. Harassment
2. Grooming

IMPLEMENTED MEASURE

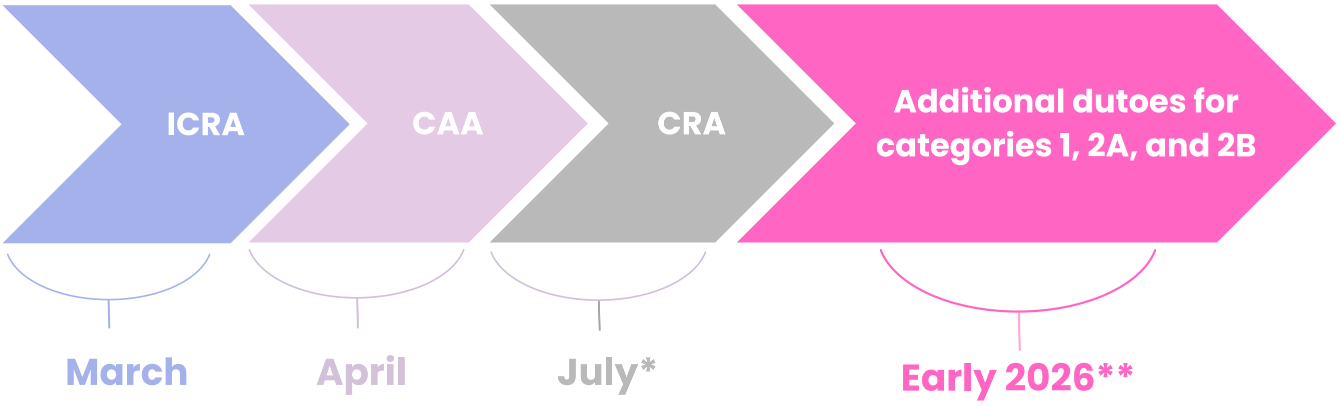
Service will collect safety metrics during on-platform testing of its matching algorithm.

Figure 3 An example of reasoning behind implementing measures.

Many lines of thinking can inform a dating service's ICRA. Here's one.

2.4 Coming soon: categorised services

The final stage of implementation (Phase 3) covers the additional duties on certain services, known as 'categorised' services. The draft codes of practice are expected from Ofcom by early 2026 at the latest, and the Government must confirm the categorisation thresholds in secondary legislation.



*Dependent on when in Spring 2025 Ofcom releases its CRA guidance
**Latest estimate

Figure 4 Timeline including additional duties

Different duties apply depending on which category a service falls into: Category 1, 2A or 2B. Right now, Ofcom has advised the Government with category thresholds dependent on mainly the number of UK users. However, there is debate on whether this should be the focus, since evidence shows that harm occurs even on smaller, high-risk services. **It is likely that many dating apps will fall under category 2B if they have more than 3 million UK users.** This means that bigger dating apps will likely have transparency reporting as an additional duty [18].

[18] To view the additional duties for categorised services, click here.

Conclusion: Find opportunity in complexity

The Online Safety Act (2023) is one of the first comprehensive regulatory frameworks for online safety, focusing on the design and operation of digital services. Unlike approaches which mandate the removal of harmful content, the Act incentivises dating services to adopt a safety-by-design approach to protect UK users from illegal harms and to safeguard children.

Due to the emphasis on systems and process rather than content, the Act expects dating services to:

01 **Think carefully about the risks their service pose**

02 **Record their decision-making process on what to do**

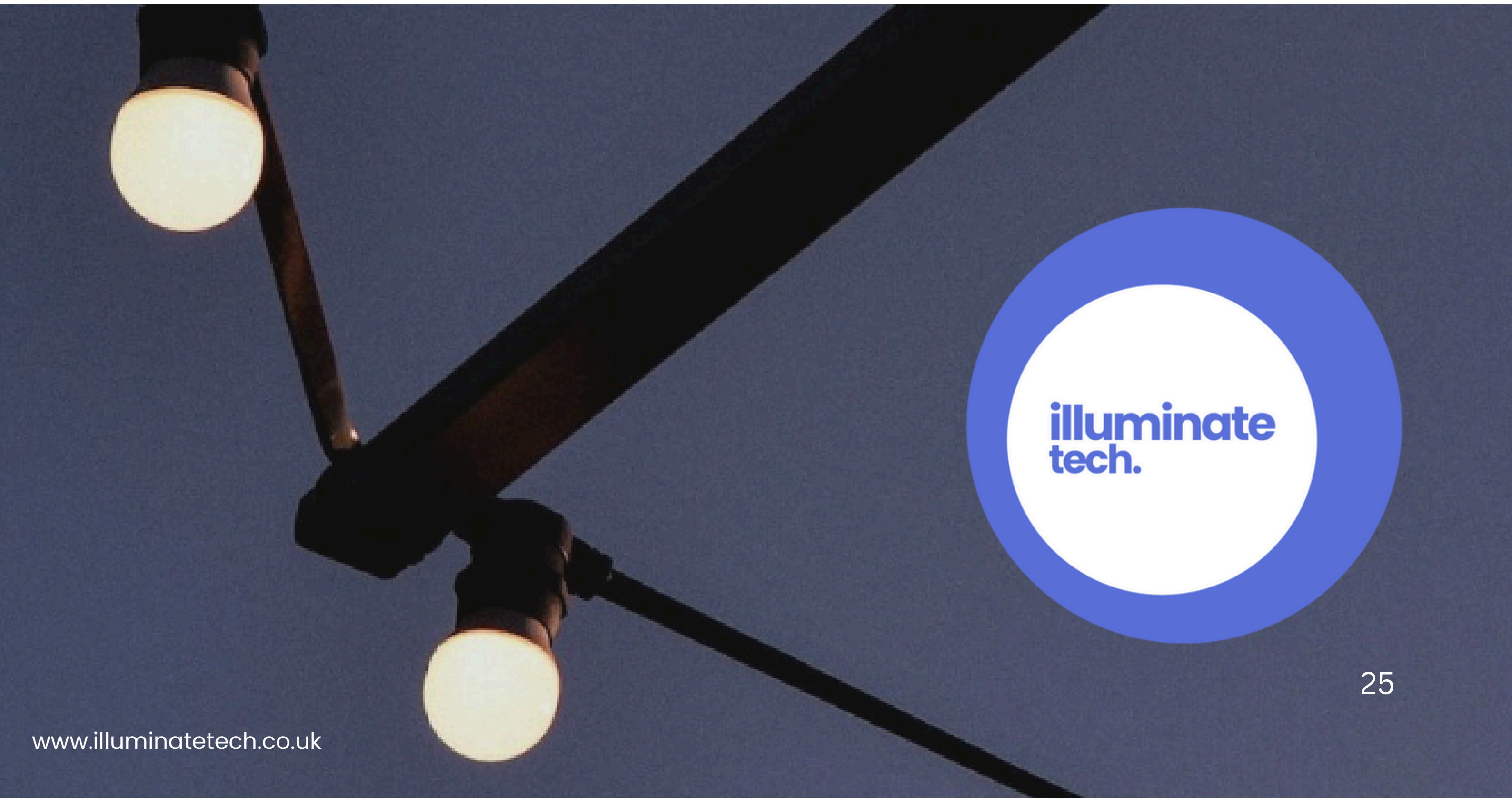
03 **Implement measures to mitigate the rtisk of harm**

04 **Introduce systems to evaluate the effectiveness of their measures**

The Illegal Content Risk Assessment (ICRA) and the Children's Access Assessment (CAA) guide platforms to identify risks and implement proportionate safety measures. We expect Highly Effective Age Assurance (HEAA) to become a standard measure across dating platforms, allowing them to effectively enforce their 18+ user condition. Finally, as the Act moves into Phase 3, larger dating platforms may face additional transparency and reporting duties.

Recent international political developments have led to some online platforms de-prioritising user safety. In response, internet users have proven willing to leave traditional apps and move to platforms that prioritise providing safe, meaningful user experiences. The UK's Online Safety Act introduces a new standard for accountability and transparency in tech platforms operating in the UK, with international implications.

Providers of dating services who move quickly to embrace this move towards transparency, build safer platforms, and implement processes to track the effectiveness of their measures will be better placed to build loyal, satisfied user bases in an increasingly volatile economic climate.



Explainable expertise.
For a better internet.

Contact

Illuminate Tech
113-115 Fonthill Rd,
London N4 3HH
www.illuminatetech.co.uk
hello@illuminatetech.com