Children first: How Ofcom's Children's code and age checks change the digital game

Client Alert | 4 min read | 07.29.25

Ofcom, the UK's communications and appointed online safety regulator, is following through on its commitment to protect children online. From 25 July 2025, Ofcom will enforce its **Protection of Children Codes of Practice** (the "Code") under the Online Safety Act 2023 - a significant milestone for digital safety in the UK.

The Code sets a new standard for safeguarding children in the digital world. It calls on online service providers to implement robust protections, whether by following Ofcom's recommended measures or documenting alternative compliance approaches. Services likely to be accessed by children had a deadline to complete a children's risk assessment by 24 July 2025, and those who have acted early to align with the Code will be best positioned when enforcement begins. Proactive preparation not only demonstrates a commitment to compliance but also helps platforms adapt more smoothly to Ofcom's evolving expectations.

The Code outlines measures for providers of online services ultimately to protect children from harmful content. It addresses governance, accountability, user controls, content moderation, and reporting. Providers must ensure these processes are in place and regularly reviewed. A key area making headlines are the Code's stringent requirements for age assurance.

Key feature of the Code: age assurance

Age checks are at the heart of the Code, requiring providers to use ***highly effective***, user-friendly, and age-appropriate design code to verify or estimate users' ages to ensure that children are protected from accessing or encountering inappropriate material. This is especially crucial for services hosting high-risk content (such as pornography or material related to suicide, self-harm, or eating disorders).

To be highly effective there must be:

1. Technical accuracy (*e.g.*, determining a user's age under test lab conditions),
2. Robustness (*e.g.*, identifying and taking feasible and proportionate steps to prevent any possible circumvention, especially methods easily accessible to children in the UK, and tested in multiple environments),
3. Reliability (*e.g.*, reproducible results if using AI or machine learning with monitoring of any outputs, evidence relied on being a trustworthy source), and
4. Fairness (*e.g.*, any elements of an age assurance process which relies on AI, or machine learning, has been trained on diverse data reflecting the target population and does not produce significant bias or discriminatory outcomes). In practice this is one of the first live examples of algorithms needing to demonstrate fairness from a legislative perspective in such an express and prescriptive manner.

There are also requirements to allow appeals to age assessments, as predictably age assurance will not always be accurate, in line with data protection rules such as those allowing individuals to correct their personal data or to challenge decisions made solely by automated means. In collaboration with the Information Commissioner's Office ("ICO"), the UK's data protection regulator, Ofcom expects age assurance and safety measures to be built around strong data protection principles from the outset.

If a provider does not implement highly effective age assurance, they must assess whether their service is likely to be used by children. If so, and where certain criteria are met, the provider is required to introduce additional safety measures to protect child users.

On the online safety horizon

Online service providers will need to prioritise compliance with Ofcom's *highly effective* age-check requirements to mitigate enforcement risks and legal exposure. Over the last couple of months, adult service providers and other platforms have committed to deploying age-checks, though what will be considered as *highly effective* remains to be seen. Businesses hosting user-generated content will also need to review and update their age assurance and content moderation practices to ensure alignment with the Codes.

Potential enforcement actions include fines of up to £18 million or 10 percent of annual global turnover (whichever higher), court orders to block access, forcing intermediaries (*e.g.*, payment processors, ISPs) to remove support, and senior managers may be criminally liable (with up to two years' imprisonment). With robust enforcement powers, Ofcom has signalled it will not hesitate so platforms should not expect leniency or delays. The upcoming Register of Categorised Services, due to be published by Ofcom in summer 2025, will also clarify which platforms face the most stringent obligations.

The protection of children is taking centre stage in the online safety discussion in the UK. For those involved in child protection or age assurance, these regulatory changes could present a valuable opportunity to support and advance online safety measures for children. Ofcom's Chief Executive, Dame Melanie Dawes, has **urged** tech firms to prioritise child safety in complying with the protection measures. As the regulatory landscape shifts, businesses who operate services that are accessible, or deemed potentially harmful, to children will need to act decisively and proactively to meet these new standards.

Contacts

Emma Wright
Partner
London D | +44.20.7413.1315
ewright@crowell.com

Grace Tang
Associate
London D | +44.20.7413.1353
gtang@crowell.com