

Protecting children and their data in the online environment

19 December 2022

Introduced in September 2020, the ICO Children's Code (Code) was aimed at tackling a lack of privacy for children online.

We have all read the tragic events surrounding Molly Russell's death in 2017; Molly had subscribed to several online sites which were not safe for children to access. The Coroner in Molly's case reported that these sites contributed to Molly's death by negatively affecting her mental health.

UNICEF estimates that one in three internet users are children; raising concerns about their privacy, mental health and wellbeing and, in particular, their use of social media.

The Code has the intention of protecting children who use, amongst other things, online messaging, content streaming, games and apps that fall under the heading of 'information society services' (ISS). It recommends that, as a default, children should have their privacy settings set to 'high' and collection of data about the user should only occur where it is necessary.

After the Code was introduced, companies like Instagram disabled targeted adverts and turned off its location trackers for those under 18. Although the Code was drafted to apply in the UK only, companies with a global reach such as Instagram applied it across their platforms. This led to other countries, notably the US (as recently as September 2022) and Ireland, drafting similar Codes.

It is likely that the UK's Code will be reviewed following one of the recommendations in the Coroner's report that the Government should review the provision of internet platforms to children, specifically that their age is verified before anyone can join the platform and material viewed by a child is retained.

Online services would need to provide safeguards based on children's ages. It is of course difficult to properly verify age but organisations should consider the risks of processing data and they should also consider the extent to which they can rely on ages provided by the children using the platform. Ironically, some commentators argue that by submitting age details, this adversely affects privacy and could increase the risk of online harm to the very children using the platforms.

Children under 13 should obtain parental authorisation. It can be easy to fool the age verification protections and opinion is divided on the impact of the Code: a consultation which closed in November 2022 that evaluated the Code found that some thought it 'inspirational' whilst others thought it 'too onerous on organisations'.

In the UK, the Online Safety Bill is going through the legislative process; it is currently at the report stage in the House of Commons. In Molly's case, the Coroner recommended legislation be enacted to ensure the protection of children and to regulate harmful content as well as the setting up of an independent regulatory body to monitor online content.

The [ICO website](#) contains useful information about children's online privacy and highlights the importance of being careful when collecting and processing children's personal data because they are far less likely to be aware of the risks involved. Consent is a potential lawful basis for processing the data, however, alternative bases should be considered as they may provide better protection. It's important to note that only children over the age of 13 can provide their own consent and specific protections are needed when using the data for marketing or creating user profiles. The privacy notices online need to be clear enough for a child to understand what happens to their data and what their rights are (which are the same as those an adult has).

We have recently dealt with some 'right to erase' cases. Right to erasure can be particularly relevant to cases where consent was given when the person was a child. One of the specified circumstances in which the right to erasure applies is when the data subject was a child

and data was collected under the lawful basis of consent .

The ICO has also provided [guidance](#) which is not a statutory code of practice but will help with compliance and demonstrate best practice.

Author

Angela Williams
Legal Director

angela.williams@brownejacobson.com

+44 (0)330 045 2785

Our expertise

Services

Child protection and safeguarding
in schools

Children's services

Data protection and privacy

Data protection guidance for
schools and trusts

Information law