The Information Commissioner's response to Ofcom's consultation on recommendations on how online platforms, broadcasters and streaming services should promote media literacy

08 December 2025

About the Information Commissioner

The Information Commissioner (the ICO) has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations 2003 (PECR) as amended by the Data (Use and Access) Act 2025.

The Information Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and takes appropriate action where the law is broken.

Our approach to this consultation response

We have engaged with Ofcom during the development of some of the documents subject to this consultation, and we welcome the opportunity to respond to the consultation in full. We stand ready to continue our engagement as Ofcom finalises the measures and guidance.

We have limited our comments to matters that fall within our data protection remit. We have not provided observations on issues such as the overall effectiveness of the recommendations, except where it is relevant to data protection.

Where appropriate, we have offered feedback on the extent to which the proposed recommendations align with data protection principles and obligations. We have also identified areas where further clarification or additional safeguards may be required to ensure compliance and protect individuals' rights.

Overarching comments

We broadly welcome Ofcom's recommendations to providers on the promotion of media literacy and recognise their potential to strengthen public resilience and confidence in the online environment.

We welcome that the draft recommendations make it clear that Ofcom expects services to comply fully with data protection legislation. We particularly value recognition in paragraph 2.15 of the consultation document that while the recommendations in the consultation may not be mandatory under the Communications Act 2003 or Online Safety Act 2023, they may intersect with or overlap with existing mandatory obligations under data protection law where services process personal data. We would welcome confirmation from Ofcom that this statement will also appear in the final published version of the recommendations with appropriate prominence. This will help ensure that both services and individuals are reminded of their legal rights and responsibilities under data protection law and underline the risks for services that do not meet compliance requirements.

We also consider that the recommendations should make it clear that to services that are likely to be accessed by children and which process children's data should also conform to the ICO's Children's code. Some of the recommendations set out in the consultation have similarities to the standards contained in the code.

These references to data protection requirements will support services navigating the requirements of both regimes and ensure that Ofcom's recommendations are situated firmly within the broader legal and regulatory landscape, helping providers to recognise both their immediate relevance and their established foundation in data protection law.

Our response to the consultation document are set out in table format and enclosed within this document.

Location	Ofcom's proposals	ICO comments
Page 3 (penultimate paragraph) consultation document and paragraph 1.8	Ofcom note that their recommendations are not legally binding and are instead guidelines for good practice, meant to help service providers understand how they can support media literacy. Ofcom state that while these recommendations are not mandatory rules, we encourage service providers to follow them. Our recommendations are intended to be proportionate, (for example, small service providers might adopt the recommendations with different actions than the largest service providers) and have relevance to a wide range of different service providers.	Given that some of the recommendations are mandatory under data protection law and the importance of this point, we suggest that Ofcom add a footnote in the highlighted areas, referencing footnote 2.15 in the final documents, to clearly state that services are expected to comply fully with data protection legislation.
Recommendation 1: Embed media literacy by design, making inclusive design choices a foundational principle in service architecture and policy		
Paragraph 4.8	As part of its recommendation to embed media literacy by design, Ofcom emphasise that service design plays a vital role in shaping user behaviour and building trust. Ofcom highlight that when users understand how their data is used and the choices they make, they can engage more meaningfully. It also emphasises that inclusive design is essential to ensure accessibility for all, including children, people with disabilities, and those with lower digital confidence. They recommend that service providers adopt and	We agree with Ofcom that people engage more meaningfully and responsibly when they understand how a service operates, particularly how their data is used and the choices they make. This aligns closely with the transparency principle under data protection law, which is central to a 'data protection by design and default' requirement. Transparency is especially important where processing is complex or involves children. Proactively respecting privacy not only meets legal obligations but can also provide a competitive advantage by building trust with the public, regulators, and business partners. We recommend that Ofcom link to the ICO's transparency guidance and data protection by design and default guidance to help services

	publish a 'media literacy by design' policy that evolves with user needs and technology. For services likely to be used by children, Ofcom stresses the importance of age-appropriate design, prioritising simplicity, safety, and clarity through default privacy settings, clear explanations, and compliance with relevant legislation.	understand how they can meet similar aims from a data protection perspective. We also agree with Ofcom's assertion of the importance of age-appropriate design for services likely to be accessed by children. The ICO's Children's code sets out how online services should appropriately safeguard children's personal data. It should be followed to ensure children's data is processed fairly and that the best interests of the child are considered in all aspects of service design, including measures to protect and support children's development, health, and wellbeing. We note that Ofcom have included a reference to our guidance in footnote 15 and believe that further information on the aims and intentions of the Children's code, as outlined above, would be beneficial.
Recommendation 2: Offer clear, meaningful choices and transparent information at key points in the service experience		
4.15	Ofcom recommend that service providers clearly inform people, at key moments in the user journey, such as during sign-up or profile creation, about the types of content available on the service (including any potentially sensitive material), as well as the use of recommender systems. It states that this should include clear explanations of what these systems do to help them understand their choices and support informed decision-making. This could be done through, for example, their terms of service, by providing clear onboarding information, through consent and transparency, prompts/reminders or accessible help on the service.	It is important to highlight that the recommendation for services to provide users with information about recommender systems at key points in the user journey overlaps with existing requirements under data protection law. Under the transparency principle, services must explain how personal data is used, including the purposes of that processing. Article 13 of the UK GDPR sets out the information to be provided when personal data is collected directly from users. Transparency is fundamental to the 'data protection by design and by default' approach. It enables individuals to exercise their rights and gives them greater control over their online experiences. In relation to informed decision-making and genuine choice, it should be noted that when consent is relied upon as the lawful basis for processing under the UK GDPR, clarity alone does not suffice. For consent to be valid, it must be freely given, specific, informed, and unambiguous, ensuring that individuals are able to exercise a genuine choice regarding the processing of their personal data.

		We therefore recommend that service providers go beyond transparent onboarding information and prompts, ensuring their consent mechanisms meet the requirements of UK GDPR. Doing so will safeguard individuals' rights and build trust in the use of recommender systems and other data driven features. Our comments on our Children's code above will also be relevant for recommender systems.
Recommendation 3: Equip people with practical tools to manage and personalise their online experiences		
4.24	Ofcom recommend that service providers provide simple, accessible tools for people to be equipped to manage their experiences during use. To support safe and informed choices, service providers should ensure it is easy to turn defaults off – but also to turn them back on again – and should prompt or remind users – especially children – of the option to re-enable protective defaults.	We agree with Ofcom's comments that high privacy settings should be enabled by default to safeguard users, especially children, and suggest that they include a footnote to the ICO's Children's code (Standard 7) that require services to set high privacy settings on by default to ensure the best interests of the child are protected, to remind services of the importance of conforming to the recommendation in order to meet their data protection obligations as well. In our Children's code, we suggest rather than simply making it easy to disable defaults, services should use positive nudges to remind children of the benefits of keeping protective settings on, ensuring transparency and reinforcing privacy as the norm.
Recommendation 5. Empower and support parents and caregivers to guide and support younger users in age-appropriate and meaningful ways		
4.33	Ofcom recommend that service providers set strong privacy and safety defaults for child accounts or profiles creation and clearly present parental controls at sign-up and other opportune moments, helping families make informed, safe choices from the outset.	We recommend that Ofcom include a footnote to remind services of the alignment between the recommendation, data protection law and our Children's code: "This aligns with the principle of data protection by design and by default. Protective settings should be on by default to safeguard users, especially children, in line with the ICO Children's Code (Standard 7). Defaults set to high privacy ensure the best interests of the child are protected.

		Services should also make positive nudges to remind children of the benefits of the default settings"
Recommendation 9. Support the media literacy of underserved and diverse audiences		
4.54	Ofcom recommend that service providers adopt inclusive design practices that address a broad spectrum of media literacy needs, especially for those most at risk. This includes using plain language, visual cues, and conducting user testing with underrepresented groups to ensure that information is clear, accessible, and meaningful.	We support Ofcom's recommendation and think it should be made clear that using clear and plain language aligns directly with the transparency requirements under data protection law. Transparency is a core principle of the UK GDPR, ensuring that individuals understand how their personal data is collected, used, stored, and shared. For further support for online services, we recommend signposting to the ICO's guidance on transparency. We recommend that Ofcom also adds a footnote to the ICO and CMA's DRCF paper on "Harmful Design in Digital Markets" when it finalises this recommendation harmful-design-in-digital-markets-ico-cma-joint-position-paper.pdf. The paper highlights how manipulative design practices in digital markets (such as default settings, misleading language, and exploitative nudges) can harm consumers by undermining privacy, choice, and competition. It sets out a joint position from the ICO and CMA, calling for stronger regulatory collaboration to curb harmful design and promote fair, transparent, and user-centric digital environments.
Privacy impact assessment		
Paragraph 5.15	As part of its privacy rights assessment, Ofcom note that Article 8 of the ECHR sets out the right to respect an individual's private and family life. It then states that some of the proposed recommendations may involve the collection and processing of personal data, such as proposed recommendations 1, 2 and 5. Ofcom does not envisage that recommendations 6, 7 and 8 involve the	As drafted, the privacy and data protection rights assessments do not take full account of the impact of the measures on data protection rights and appear to conflate legitimate expectations of privacy under Article 8 of the European Convention on Human Rights (ECHR) with data protection rights. We suggest it may be helpful for these to be considered separately. It is not clear from the assessment that Ofcom has considered the range of data protection impacts that can arise from this processing.

	collection or processing of personal data for their implementation.	
Paragraph 5.16	Ofcom make clear that it expects services to comply fully with data protection legislation, including the UK GDPR and relevant guidance from the Information Commissioner's Office (ICO). Ofcom states that any potential interference is mitigated by the non-mandatory nature of these proposed recommendations and the strong emphasis on privacy by design and default. For example, services are encouraged to use non identifiable usage patterns, contextual indicators, or aggregated behavioural signals to inform design decisions, rather than relying on direct personal data collection. Therefore, we consider any potential interference with privacy rights to be minimal where these proposed recommendations are adopted as intended.	It is important to stress that compliance with the transparency principle and other core requirements of data protection law remains a legal obligation, not optional. While we recognise the intention to minimise interference with privacy rights, we would emphasise that the overarching safeguard lies in strict adherence to data protection law, with privacy-by-design and by-default embedded throughout service design. Our understanding of this assessment is that Ofcom appears to conclude that any risk to individuals' rights is mitigated because the recommendations are optional and designed to embed privacy from the outset. However, this is not stated explicitly. We interpret Ofcom's comment to mean that, where possible, services could use anonymised data to achieve the intended outcomes of the recommendations by reducing the collection of personal data. We suggest Ofcom make this point explicit and direct services to the ICO's guidance on anonymisation. This would help organisations understand anonymisation techniques, their strengths and limitations, and when they are appropriate to use.