The Information Commissioner's response to Ofcom's consultation: A safer life online for women and girls

23 May 2025

About the Information Commissioner

The Information Commissioner 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). 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. The ICO's strategic objectives include safeguarding and empowering people and empowering responsible innovation.

The Data (Use and Access) (DUA) Bill was introduced to Parliament on 24 October 2024 and is expected to become law later in 2025. When the Bill becomes law, it will make changes to UK data protection law. This response, including all referenced links, has been prepared in accordance with the applicable legal framework at the time of writing. If any of the provided links become inaccessible, Ofcom is encouraged to consult with the ICO for the most up-to-date guidance.

ICO and Ofcom collaboration

As the bodies responsible for regulating data protection and online safety in the UK, the ICO and Ofcom share a commitment to protecting people online. We published a joint statement in 2022, which set out our overall vision of ensuring coherence across online safety and data protection requirements and promoting compliance with both regimes.

In May 2024, we deepened our collaboration and published a second joint statement, explaining how we intend to collaborate on supervision and enforcement on issues that are relevant to both regimes, including the protection of children online.

The joint statements recognise that online safety and data protection interact in a variety of ways. They set out our overall ambition to ensure coherence across online safety and data protection requirements and promote compliance with both regimes. The ICO recognises the importance of consistent messages to businesses, and we will continue working hand in hand with Ofcom to ensure that all users can enjoy a safe and privacy-respectful online experience.

Compliance across the data protection and online safety regimes

The ICO is supportive of the online safety regime and its objective to make the UK the safest place in the world to be online. We recognise Ofcom's ambition to improve the safety of women and girls online. We have engaged with Ofcom during the development of this consultation, and we welcome the opportunity to respond to the consultation in full. We stand ready to continue our engagement with Ofcom as it finalises its guidance.

The Information Commissioner has made it clear that he expects regulated services to fully comply with data protection law when implementing Ofcom's recommended code measures or following its online safety guidance. We are pleased that Ofcom has incorporated references to data protection law in several chapters of the draft guidance. Given that most good practice steps are likely to involve the processing of personal information, we believe a general reminder of the need to comply with data protection law at the start of the guidance would help ensure that services take the necessary steps when handling personal information. We suggest that the final guidance refers services to the ICO's guide to UK GDPR which offers guidance on carefully assessing the necessity and proportionality of personal information processing, determining the minimum amount of personal information required to achieve the intended purpose, and selecting the most appropriate lawful basis for processing.

The first principle of data protection law requires data processing to be lawful, fair, and transparent. Services must identify a lawful basis in order to collect and process personal information. There are six lawful bases for processing set out in Article 6 of the UK GDPR, one of which is the 'legal obligation' basis (Article 6(1)(c) UK GDPR) which is available if services need to process personal information to comply with a common law or statutory obligation. The guidance describes the status of the good practice steps in various ways but on our reading it is ambiguous about how the good practice steps relate to compliance with the OSA duties. This creates an uncertainty about whether legal obligation could be an appropriate lawful basis for personal information processing that is carried out when following the good practice steps.

We would therefore welcome more clarity in the final guidance about the status of the good practice steps and their relationship to compliance with the OSA duties. This would provide services with clearer information to enable them to make an informed choice about whether the legal obligation lawful basis is appropriate for their processing.

For the avoidance of doubt there are other lawful bases in Article 6 UK GDPR that could be relevant for the processing associated with the good practice steps. The final guidance could usefully refer services to the ICO's guidance on lawful bases and remind them that under data protection law they will need to ensure that they have a lawful basis for their processing under Article 6 UK GDPR.

Given the consultation documents' focus on girls' safety, Ofcom should be aware that under data protection law "children merit specific protection[1]" in respect of the processing of their personal information. The ICO's Age Appropriate Design Code (the Children's code) explains how service providers can ensure that they appropriately safeguard children's personal data. Signposting to the ICO's Children's code in the final guidance will help service providers who are subject to compliance with both OSA and data protection law.

Foundational steps and ICO comments

Across the nine action areas of the guidance, we recognise that the foundational steps are derived from Ofcom's Codes and risk assessment

[1] Recital 38 - Special Protection of Children's Personal Data - General Data Protection Regulation (GDPR)

guidance, which have been outlined in its work on illegal harms and the protection of children.

As the ICO has previously provided consultation responses on illegal harms and the protection of children, this response will focus on the good practice recommendations and the draft case studies presented in Annex A (the draft Guidance). We encourage Ofcom to consider our previous consultation responses to gain further insights into our perspectives on the foundational steps within this consultation document.

Consultation questions

Question 3: Do you have any comments about the effectiveness, applicability or risks of the good practice steps or associated case studies we have highlighted in Chapter 3, 4 and 5? Are there any additional examples of good practices we should consider? Please provide evidence to support your comment.

Chapter 3: Taking responsibility.

In this chapter, we acknowledge Ofcom's view that, to address online gender-based harms, comprehensive governance and accountability processes are required. The draft guidance explains that this is considered necessary to help integrate online safety into design choices, while ensuring compliance with risk assessment duties under the OSA. This approach aligns with the accountability principle under the UK GDPR, which is a key requirement that ensures organisations are complying with data protection law and demonstrating their compliance to the ICO as the data protection regulator.

We consider that the good practice steps outlined in this chapter are likely to involve the processing of personal data. Therefore, we suggest that the final guidance reminds services that, where processing of personal information is taking place, they must comply with data protection law requirements, particularly the data minimisation principle. Whenever possible, services should anonymise or pseudonymise personal information to reduce the risk of it being linked to an identifiable individual.

Our anonymisation guidance will be a valuable resource in supporting services through this process, and we believe that signposting it in the

guidance could benefit service providers. In the consultation document (page 27, paragraph 2.56), Ofcom referenced our plans to publish this guidance in Spring 2025. We therefore take this opportunity to inform Ofcom that this guidance has now been finalised and is available for services on our website.

Action 2: Risk assessments

Within the good practice steps in action 2, we note that Ofcom encourages services to adopt approaches that enhance their understanding of users' experiences to provide valuable insights into how design choices may pose risks for women and girls. This includes engaging with survivors, victims, and users with protected characteristics alongside their risk assessment duties.

Personal information recorded through these approaches may constitute special category data, under Article 9 of the UK GDPR. Special category data includes details about a person's race, ethnicity, sexual orientation, or disability, all of which require additional legal protection under data protection law. Additionally, information about a perpetrator identified by a victim or survivor may qualify as criminal offence data under Article 10 of the UK GDPR.

The ICO has developed guidance for services regarding special category data and criminal offence data. In order to support services complying with both regimes, service providers seeking to implement these measures should be encouraged to consult our guidance to ensure compliance with data protection law. This guidance will be particularly valuable for service providers aiming to implement measures like those described in Case Study 5 of the consultation, where Ofcom offers an illustrative example of conducting user research, such as surveys, involving abuse victims and survivors.

We also note in this same action point that Ofcom has stated that it is good practice for services to gain insights into how their design choices might create risks for women and girls through conducting impact assessments, including on privacy (3.19d)). Given the reference to impact assessment for privacy, we would welcome clarification in the guidance that the proposed good practice step is separate from existing obligations to conduct a Data Protection Impact Assessment (DPIA) under data protection law.

Conducting a DPIA is a legal requirement where services undertake processing of personal information that is likely to result in a high risk to individuals. This includes certain specified types of processing, and the ICO has developed screening checklists to help determine when a DPIA is necessary.

Action 3: Be transparent about women and girls' online safety.

In this action point, we welcome the recognition of platforms' responsibility to exercise caution when sharing or providing personal information as part of transparency reporting obligations, to ensure compliance with data protection laws.

We also welcome Ofcom's suggestion to minimise the sharing of personal information that could put individuals at risk (for example, by using aggregated data) so that only necessary information is shared. Where this level of data provides sufficient transparency and achieves the intended purpose, it should be used. This approach aligns with the data minimisation principle, ensuring that only necessary data is shared. It is important to note however that aggregated data may still be personal data where individuals remain identifiable (which means that data protection law will continue to apply).

Within the good practice steps outlined in this chapter, we note that Ofcom refers to service providers sharing existing data on the prevalence of online gender-based harms, including user reports and their outcomes. We welcome the recognition in the guidance that this information must be collected and managed in accordance with data protection law. The links to our UK GDPR guidance included in Chapter 3 will help platforms understand controller-to-controller data sharing. However, we also encourage Ofcom to include a link to our data sharing code of practice in the guidance, which includes case studies on secure data sharing and outlines the necessary steps that service providers will need to take to effectively demonstrate transparency and accountability. This includes adopting best practices such as establishing a data sharing agreement where necessary.

Chapter 4: Preventing harm.

We welcome Ofcom's objectives to prevent online harms by encouraging services to adopt proactive approaches and robust product testing to

enhance safety features. We support the initiative for online services to implement stronger defaults for interactions, privacy, and geolocation, and we welcome the references to relevant ICO guidance within this chapter.

Action 5: Set safer defaults

The ICO's Children's Code employs a similar approach to the good practice steps within this chapter when protecting children's data rights online. The ICO's Children's Code requires online services to:

- implement high privacy settings for children by default unless services can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child (standard 7)
- disable geolocation by default unless there is a compelling reason for enabling it, taking account of the best interests of the child (standard 10) and
- avoid using nudge techniques to prompt children to share unnecessary personal data or turn off privacy protections (standard 13)

Ofcom's good practice steps within this action point also align with our guidance on Article 25 of the UK GDPR, which requires systems, services, and practices to prioritise the safeguarding of personal information by creating a 'privacy by design and default' approach. By setting children's accounts to 'high privacy' by default, service providers can ensure that personal information is only shared when users actively adjust their settings.

This approach aligns with Ofcom's case study 9, which includes a footnote referencing our Children's Code and advocates for limiting location-sharing opportunities, disabling geolocation by default, and providing clear warnings when location tracking is active. These measures contribute to the online safety of women and girls and enhance the protection of their personal information

Bundled privacy settings

Transparency for users

In this chapter, we note that Ofcom has suggested bundling privacy settings together to help reduce the time and effort required from users as it is suggested that users can be overwhelmed by too many options when creating a profile, meaning they disengage from making decisions. Ofcom also references a paper ('Active Online Choices: Designing to Empower Users') from the Behavioural Insights Team (Annex A, footnote 166) that suggests choice bundles can help users make informed choices.

While bundling privacy settings may seem time-efficient, it is important to recognise that this approach could increase the risks of users not being fully informed about how their personal information is processed or the significance of the choices they make regarding their data. If transparency information is vague or non-specific, users may struggle to grasp how their data is used, shared, or processed. Article 12 of the UK GDPR requires controllers to provide information about data processing in a concise, transparent, intelligible, and easily accessible format, using clear and plain language.

To ensure compliance with both regimes, we recommend that Ofcom clarify to service providers that they must meet their data protection obligations if considering implementing bundled privacy settings. Specifically, they should adhere to the transparency principle outlined in Article 5(1)(a) of the UK GDPR, as well as the requirement to provide individuals with specific privacy information set out in Articles 13 and 14.

Signposting the ICO's guidance on the right to be informed within this good practice step will help service providers understand the necessary measures to ensure users are clear on how their data is used.

Valid UK GDPR Consent

To avoid compliance risks, service providers should also be reminded that if they rely on consent as a lawful basis for the processing of personal information for privacy settings under Article 6 of the UK GDPR, that consent must be freely given, specific, informed, unambiguous, and separate from other terms and conditions.

The ICO and CMA's joint paper on harmful design warns that bundled consent is more likely to be invalid than granular consent options, as it often lacks specificity and fails to ensure users are fully informed—potentially violating the "lawfulness" requirement under Article 5(1)(a).

The ICO's consent guidance also emphasises the importance of offering granular consent options for different processing purposes, unless doing so would be unduly disruptive or confusing. At a minimum, consent requests must clearly cover all purposes for which consent is sought, be distinguishable from other matters, and allow users to withdraw consent at any time.

To support service providers, we suggest the inclusion of links to the ICO's guidance on individuals' right to be informed, valid GDPR consent, and our joint paper on harmful design within this good practice step.

Account security and account access

The ICO welcomes the additional steps related to account security within this section, particularly the use of two-factor authentication (2FA). This aligns closely with our guidance on data security, where 2FA is included as one of many measures organisations can implement to minimise the risk of a personal data breach.

We note that, as part of the good practice steps outlined in this chapter, Ofcom has recommended that service providers inform account owners about which individuals are currently connected to their account (4.29(e)). Services must ensure that such data processing is adequate, relevant, and limited to what is necessary, in compliance with data protection law. Our guidance on data minimisation may serve as a valuable signposting resource for services considering the implementation of this good practice step.

User verification

Within action 5, the ICO recognises that Ofcom has identified allowing users to verify their identity as a good practice step for service providers to enhance accountability and reduce the online disinhibition effect. We acknowledge Ofcom's view that identity verification may be beneficial in certain circumstances, but we consider that it may also present significant privacy concerns, particularly for survivors and victims. To support services seeking to implement user verification methods, Ofcom is encouraged to direct service providers to the ICO's guide to UK GDPR to ensure their approach is necessary, proportionate, and compliant with data protection law. Services should consider the data protection

implications of restricting anonymity for users, including identifying and mitigating risks of harm or other detriment to users. We will further expand upon this in our response to case study 14 (page 13 of this document).

Action 6: Reduce the circulation of online gender-based harms

We recognise that Ofcom has highlighted the importance of continuous improvement in automated content moderation systems (Annex A, 4.43) . This aligns with our recommendations and expectations under data protection law, particularly regarding the fair treatment of users' data.

We expect services to regularly review their use of personal information in moderation processes to minimise the risk of unfair outcomes for users.

To support services navigating both regulatory regimes and looking to implement these steps or the associated case study (15), a link to our content moderation and data protection guidance within this chapter will help them to ensure they are complying with data protection law when using content moderation technologies and processes. In particular, it will help them determine whether they are making solely automated decisions within their content moderation systems and whether these decisions are likely to have legal or similarly significant effects on users. If such conditions apply, the additional provisions of Article 22 of the UK GDPR will govern the data processing.

Chapter 5: Supporting women and girls

Action 8: Enable users who experience online gender-based harms to make reports

The ICO notes that one of the good practice steps suggested by Ofcom in this chapter involves service providers incorporating user feedback on their reporting process. Where a user engages with a service provider as part of this process, there may be a possibility that they could exercise

their data protection rights under UK GDPR at the same time. For example, a user may complain about certain content on the platform and request its removal. This may qualify as a valid 'right to erasure' request under UK GDPR, which must be addressed within one calendar month.

If the user considers that their request has not been fulfilled or they are dissatisfied with the service provider's response, they will have the right to escalate their complaint to the ICO. To help service providers avoid potential compliance issues under data protection law, our guide on individual rights could serve as a valuable resource. By including this link within the guidance, services can effectively identify such requests and take the necessary steps to ensure compliance.

Incident reporting

Within this action, we also understand that Ofcom has identified additional good practice steps that introduce a tailored process for users reporting online gender-based harms to services. This includes allowing users to report incidents of abuse, including abuse that happened on another service or offline, which can provide the necessary information for services to take appropriate action. Services will need to fully comply with their data protection obligations if implementing this step.
We have provided additional comments for case study 23 in the next section, where we discuss data protection considerations related to reporting offline behaviour or incidents on another service.

Action 9: Take appropriate actions when online gender-based harms occur

The ICO welcomes Ofcom's inclusion of our content moderation guidance within this action, which supports the recommended good practice steps for persuasion, removal, and reduction. For clarity, it may be beneficial to remind services here that our guidance applies to all forms of moderation. We therefore expect services to adhere to data protection laws and consult our guidance when analysing user-generated content (in any format, including voice moderation) and implementing corresponding moderation actions, relevant to the foundational or good practice steps within the guidance. These actions may include removing content, restricting user access to specific features, reducing content visibility, or providing users with nudges and warnings.

Comments on Ofcom's case studies highlighted in chapters 3,4 and 5

The ICO notes from the consultation documents that Ofcom intends the case studies in chapters 3, 4, and 5 to be illustrative only, providing practical examples of how service providers could take action rather than serving as instructions or directives for in-scope services. While we have referenced some case studies above, we note that the nature of certain case studies could create confusion for services complying with both regimes or pose potential compliance risks under data protection law if replicated in full. We have addressed these issues separately below; however, it would be beneficial for Ofcom to remind services that, as data controllers, they remain accountable for their obligations under data protection law when implementing any of the steps set out in the guidance, including if they implement the steps as set out in the case studies.

Case Study 4 - Gender-sensitive risk assessments

The case study notes that service providers often collect demographic data about users, for example for advertising purposes or to improve users' experiences, and can also sometimes make inferences on the basis of user behaviour. We are pleased that the draft guidance notes that when considering the use of personal information, service providers must consider privacy rights and comply with their duties under UK GDPR, particularly around the data protection principles.

We take this opportunity to remind Ofcom and service providers that demographic data collection for advertising or user experience improvement is frequently facilitated through storage of and access to information on users' devices, including via the use of cookies and similar technologies which are subject to the Privacy and Electronic Communications Regulations (PECR). Services engaging in such practices must ensure compliance with PECR and UK GDPR, including obtaining UK GDPR standard user consent where required. Accordingly, there is benefit for the guidance to direct services to our draft guidance on the use of storage and access technologies, PECR and broader UK GDPR guidance and resources to promote compliance across both regimes.

Case study 11 – Gender recommender systems

We note that, to address the challenges identified by Ofcom regarding gendered bias and disinformation in GenAI chatbots, this case study explores the potential for services to adopt gender-sensitive strategies. These include auditing algorithms to identify and rectify gender bias and

retraining them to detect and address gender-based harms, with consideration for intersectional factors.

We wish to draw Ofcom's attention to our guidance on AI and fairness which may be beneficial to services when implementing such measures. Although not specific to recommender systems, this guidance highlights similar risks that present under data protection law and sets out a clear methodology for auditing AI applications.

Case Study 14 – Uploader Verification

We note that Ofcom has identified providers of adult content services as being at heightened risk of hosting non-consensual intimate content due to the nature of these platforms. Where a service provider identifies it is at risk of hosting nonconsensual intimate content, case study 14 suggests several measures to mitigate this, including uploader verification and consent verification. Uploader verification may involve requiring individuals to verify their identity by providing their full legal name, date of birth, a matching government-issued photo ID, and a live face scan to upload content. For consent verification there is a suggestion in the case study that service providers can use facial recognition and nudity detection to block uploads of content if the uploader cannot provide proof of consent. The case study also suggests that removal of historic videos could be removed from unverified accounts.

We understand that restricting anonymous users can help reduce the risk of harmful content being shared, as it makes it harder for individuals to post abusive or non-consensual material without accountability. We also understand that consent verification can help to prevent intimate image abuse.

However, for service providers considering identity verification steps, a careful assessment of the data protection implications and legal requirements is essential- including consideration of the necessity and proportionality of the personal information processing and whether less intrusive options could be used. Services that choose to follow this step should ensure that they take a data protection by design and default approach to their processing ensuring that necessary safeguards are integrated to protect the rights and freedoms of users.

Services must also determine the appropriate lawful basis for processing personal data. If relying on consent for identity verification, they must

ensure it meets the UK GDPR standards for validity. In many cases, consent may not be a suitable legal basis, as restricting access for those who do not provide their data undermines the concept of freely given consent.

The ICO is concerned that services may misinterpret the suggestions in this case study as a best practice for verification or the best way to execute this good practice step within action 7, potentially leading to excessive data collection for identity or consent verification purposes. The guidance should therefore clarify that identification and consent verification measures must be compliant with data protection law. Key principles such as purpose limitation, data minimisation, and storage limitation must be followed—particularly when processing special category data like biometric face scans to uniquely identify a person.

We would encourage service providers to consider a range of options for their service before determining whether the proposed approaches set out in the case study are the appropriate and proportionate means of implementing the good practice step in the context of their specific service. This would help them to demonstrate that their personal information processing is necessary and proportionate.

To ensure that service providers can implement the steps within action 7 without facing any risks of non-compliance with data protection laws, we suggest including links to relevant ICO guidance within the case study. This would help service providers navigate data protection requirements, reduce unnecessary data collection, and minimise the risk of breaches, aligning with Ofcom's broader goal in Chapter 4 of ('preventing harm').

In relation to the suggestion that services could use facial recognition and nudity detection to block uploads of content if the uploader cannot provide proof of consent, we would welcome more detail in the final guidance about how this could work in practice. While the consultation document notes that Ofcom is aware of several pornography services currently deploying similar techniques, no further details are provided. With identity verification, service providers that choose to follow this step should ensure that they take a data protection by design and default approach to their processing ensuring that necessary safeguards are integrated to protect the rights and freedoms of users.

Case study 23 – Reporting off service behaviour

The ICO acknowledges Ofcom's conclusions that online gender-based harms, such as stalking and harassment, often form part of a larger pattern of abuse and that reporting systems, like the one outlined in this case study, can play a crucial role in helping survivors and victims' flag harmful behaviours beyond the digital space. We also note that this could enable platforms to take action against perpetrators, preventing ongoing abuse and making online environments safer for women and girls.

However, the case study raises potential data protection considerations and we would therefore suggest that the final guidance reminds services of the need to comply with data protection law when implementing the good practice step and signposts to relevant ICO guidance. Services that choose to follow this step should ensure that they take a data protection by design and default approach to the processing ensuring that necessary safeguards are integrated to protect the rights and freedoms of users. This includes clearly defining and communicating the purpose of collecting reports on harmful off-service behaviour, establishing a lawful basis for processing such data, and adhering to the principle of purpose limitation. Depending on the nature of the data reported, service providers may be processing criminal offence data. It is therefore crucial that platforms understand the responsibilities associated with handling such sensitive information. We recommend signposting services to our guidance on criminal offence data to ensure compliance and to safeguard users.

Equally important is recognising that all individuals involved in these reports—including survivors, reporters, and alleged perpetrators—retain their data protection rights. This includes access to their data, the ability to request corrections, and, in certain cases, the right to object or request erasure. Service providers must have robust processes in place to handle these requests fairly and efficiently.

Furthermore, fairness in data processing is essential, particularly if automated systems are used to analyse reports or determine enforcement actions. Any use of technology for this purpose must be transparent and free from bias. Our guidance on UK GDPR principles and automated decision-making and profiling can help platforms implement these measures responsibly.

We also consider that the suggestion that service providers "investigate" reports of off-service behaviour should be clarified, as it could otherwise

incentivise service providers to carry out disproportionately intrusive checks.

By taking a data protection by design and default approach to the good practice step, services can demonstrate their commitment to protecting women and girls online while ensuring data protection and privacy safeguards are built in. Outlining the benefits and risks will help service providers build systems that are both effective in protecting women and girls online and compliant with both online safety and data protection laws.

Concluding remarks

We look forward to continuing to work closely with Ofcom to achieve alignment and maximise coherence between our regimes and promote compliance.