Information Commissioner's response to 'Growing up in the online world: a national consultation'

Summary

Children face real and evolving risks online, some driven by how their personal information is used. We welcome the government's consultation on how to address them most effectively.

As recognised in the UK General Data Protection Regulation (UK GDPR), children merit specific protection with regard to their personal information. Their best interests should be a primary consideration in the design of online services.

The Information Commissioner's Office's (ICO) longstanding commitment to protecting children's personal information is reflected in our world-leading Age Appropriate Design Code (Children's code). This sets clear expectations for online services to protect children's privacy by default. Our associated strategy combines engagement, research, support for parents and carers and regulatory action to drive conformance and reduce risk. This includes:

- supporting organisations to make necessary changes;
- taking formal action where needed;
- drawing on research such as Children's Data Lives;
- working with civil society and representative groups; and
- helping parents and carers through our Switched on to Privacy resources.

We can use our existing powers to hold social media and video sharing platforms to account where they are not adequately enforcing their own minimum ages and are processing children's personal information. While there is no current statutory minimum age for social media use, most major platforms set a minimum age of 13 in their own terms. Where services have a minimum age, they must ensure that children below that age are not accessing those services. Failure to do so risks unlawful processing of children's personal information under the UK GDPR and exposes children to harms. We have demonstrated that we are willing to

take formal action where services are not enforcing their own minimum ages, as demonstrated by recent fines against Reddit and Imgur. We have also been clear in our open letter with services relying on weak age gates, such as self-declaration, that they need to do more.

Data protection obligations apply irrespective of any minimum age or service restriction. Raising the age at which users can consent to organisations using their personal information (the digital age of consent) or placing age gates on services will not reduce an organisation's duty to process personal information fairly and transparently.

Raising the digital age of consent on its own will not amount to a social media ban. Organisations can, and often do, rely on legal bases other than consent to process user information, including children. Where organisations use consent as their lawful basis, data protection law does not prevent processing of children's data under that age. It simply requires parental authorisation for such processing to take place. Increasing the age of digital consent would also have implications for services beyond social media platforms.

Any 'social media ban' will need to be underpinned by a clear requirement for robust and privacy-preserving age assurance. We recognise that all age assurance methods involve the processing of personal information. Organisations can process personal information for age assurance, as long as the method used is necessary, proportionate to the risks and complies with data protection legislation. If the intention is to ensure that children under a certain age are prevented from accessing a platform, then a clear requirement for highly effective age assurance at sign up would ensure no ambiguity in expectations.

Despite seeing wide-ranging improvements in the ways in which platforms process children's personal information, some platforms continue to dispute our position on the potential harm caused by processing children's data on certain online services and challenge our attempts to address them. Where platforms are not going to change voluntarily and we need to take regulatory action, amending data protection appeals processes so that cases involving enforcement or monetary penalty notices start in the Upper Tribunal, rather than the First Tier, and removing the full merits right of appeal against information and assessment notices would help to achieve quicker and more efficient regulatory outcomes, and swifter case law to improve certainty.

Design choices matter. We support government in taking an evidence-based approach when considering potential restrictions on children's access to specific functionalities, including those incorporating compulsive design.

Regulatory coherence across data protection law and the Online Safety Act (OSA) as well as any future statutory measures is essential. Regulatory certainty is the best way to drive improvement for industry and achieve high standards of protection for children.

Introduction

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the Department for Science, Innovation and Technology's consultation "Growing Up in the Online World: A National Conversation".

We strongly support the government's ambition to ensure that children experience a safe, empowering and developmentally appropriate online world. As the UK's independent data protection regulator, we have a statutory obligation to ensure that organisations process children's personal information fairly, lawfully, transparently and in line with data protection law. Our Children's code provides a framework for the safe use of children's personal information.

Children's data rights, privacy and development should sit at the heart of policy decisions. Our response to this consultation emphasises how we think the government's policy proposals can align with data protection law and principles. We also emphasise the importance of ensuring coherence in any policy response across data protection and online safety regimes.

We look forward to continued engagement with government and Parliament, fellow regulators and wider stakeholders to ensure that policy decisions are evidence-based, practical and aligned with children's long-term digital rights and wellbeing.

Our role and mission

We have responsibility for promoting and enforcing the UK's information rights framework including:

- UK GDPR;
- Data Protection Act 2018 (DPA);

- Freedom of Information Act 2000 (FOIA);
- the Environmental Information Regulations 2004 (EIR); and
- Privacy and Electronic Communications Regulations 2003 (PECR).

We are independent from the government and uphold information rights in the public interest, promoting openness by public bodies and organisations and data protection for people. We do this by providing guidance to people and organisations, solving problems where we can and taking appropriate action where the law is broken.

The scope of our response

This consultation considers changes to data protection legislation and wider legislative change to address broader concerns about children's online safety and wellbeing.

We have structured our response to:

- explain the role data protection law currently plays in protecting children online and in age assurance;
- highlight some relevant ICO regulatory activity;
- provide our comments on the proposal to amend data protection law;
- explain the data protection implications of the wider legislative changes; and
- provide further general comments on the consultation.

We have not provided an answer to all the consultation questions or an opinion on whether the proposed wider changes should go ahead. We have instead limited our response to matters within the scope of our data protection remit.

The role of data protection in protecting children online and age assurance

Data protection law applies whenever providers of online services use children's personal information. For example, when they:

- collect a child's personal information to set up an online account for them;
- recommend products or online content based on a child's use of a service;

- track a child's location; or
- track a child's progress in an online game.

Social media platforms use children's personal information in their systems, including those with recommender systems. Our Children's code contains 15 standards that online services likely to be accessed by children should follow to ensure they are complying with their obligations under data protection law.

Data protection law does not set a 'minimum age' for children to use services. However, it does require organisations to use children's personal information fairly, lawfully and transparently. Our Children's code explains that, in practice, this will include:

- services upholding their own published terms, policies and community standards, including any age restrictions they have imposed; and
    - implementing age assurance measures that are proportionate to the risks to children from the use of their information; or
    - applying the standards of the Children's code to all users regardless of age, where appropriate.

Under data protection law, organisations must have a lawful basis to process personal information fairly and lawfully. There are a range of lawful bases that that organisations can use to process children's data, including legitimate interests and consent. If online services choose to rely upon consent[1] as their lawful basis, only children over the age of 13 can provide this consent.[2] For children under the age of 13, someone with parental responsibility must give or authorise consent. Services must make reasonable efforts to verify that the person providing consent holds parental responsibility.[3]

The digital age of consent requirements won't apply if a service chooses to rely upon another lawful basis for processing a child's personal information. Our experience is that most online services do not rely on consent as the lawful basis for most of their processing, instead choosing

[1] For the avoidance of doubt, consent as a lawful basis under data protection law is distinct from general agreement to using a service.
[2] See Article 8 of the UK GDPR
[3] See Article 8 (2) of the UK GDPR

to rely on legitimate interests. Consent is unlikely to be the most appropriate lawful basis for a service's processing activities.

If a service includes a minimum age as part of its terms of service, ie many social media platforms already self-impose a minimum age of 13, then that service will have no lawful basis for processing children's information who are under that minimum age. As such, services should look to prevent access to children under the minimum age to avoid unlawfully processing their information. This would also avoid any associated risks of harm to underage children accessing a service that has not been designed for them.

Services still need to ensure they are compliant with data protection law, even if they do allow children access and have a lawful basis for processing their personal information. This includes higher protection matters under article 25 of UK GDPR, which recognise that children merit specific protection in relation to the use of their personal information.

While we regulate the use of children's personal information online, Ofcom is the regulator for the OSA. The OSA requires online service providers within its scope to take measures to protect their users from illegal content and content harmful to children. We work closely together to ensure online services both protect children's data and protect children from harmful content and interactions, creating a safer digital environment. We have set out our approach to working together in a series of joint statements.[4]

Our regulatory activity

We deploy a varied regulatory toolkit to help tackle online data protection harms and create a safer space for children to access digital services. We do this through:

- our guidance;
- raising awareness of information rights with the public;
- engaging with services to make changes voluntarily;
- taking formal enforcement action including issuing fines; and
- extensive regulatory cooperation with Ofcom, the Digital Regulators Cooperation Forum (DRCF) and others.

[4] See the latest of these statements at ofcom-ico-joint-statement.pdf

A key regulatory focus has been delivering our Children's code strategy looking at social media and video sharing platforms. Supporting parents and children to navigate the online world is a key component. On 7 April 2026 we launched a national 'Switched on to Privacy' campaign designed to increase parental knowledge about the use of children's personal information online and encourage conversations to enable both parents and children to make more informed choices.

We are also focused on ensuring organisations take action to build in appropriate protections by design and default. Our strategy has focused on approaches to age assurance, the use of recommender systems, improving default protections for children and using information about children under the age of 13. We have seen significant improvements across these areas and are now expanding our children's strategy to address mobile games.

Recommender systems are algorithmic processes that use personal information and profiling to learn user preferences and interests to suggest or deliver content. In March 2025, we launched an investigation into TikTok's processing of children's personal information in recommender systems, noting the concern that platforms using recommendation algorithms to personalise content expose children to wellbeing harms (including harmful content).

We issued an information notice to TikTok to gather the information required to progress our investigation. However, TikTok appealed against the notice on the grounds that it sought information related to processing of personal information for artistic, academic, literary and journalistic purposes (the 'special purposes'). TikTok is not required to provide any of the requested information or documents, pending determination or withdrawal of the appeal. We are defending the appeal.

This follows our fine to TikTok in 2023 for infringing the UK GDPR consent requirements (article 8), transparency obligations (articles 12 and 13) and, by implication, failing to ensure processing was fair, lawful and transparent (article 5(1)(a)). The fine was also appealed on the grounds of special purposes and the case is ongoing in the courts.

We have also issued fines to Reddit and Imgur for failing to stop children under 13 accessing their services, leading to an unlawful use of their information. Reddit has appealed the fine and this litigation remains ongoing.

Whilst platforms have made significant changes in some areas, more needs to be done. For example, some platforms continue to use self-declaration to uphold their own age restrictions or to ensure that the right protections are afforded to children. Given that self-declaration is easy to circumvent, this means that it is likely that services are unlawfully processing the data of children under their minimum age.

We have therefore called on organisations to ensure they are enforcing the minimum ages on their platforms robustly by implementing an effective age gate. We issued an open letter and wrote directly to TikTok, Snapchat, Facebook, Instagram, YouTube and X. We are coordinating with Ofcom on this work and, if necessary, will consider further regulatory interventions, using our formal powers where appropriate.

We continue to take steps to drive forward improvements, both through our own action and in collaboration with others. However, the pace and breadth of change is impacted by the speed at which data protection cases can progress through the courts and the significant resource implications of taking enforcement action. As a whole economy regulator, we have to prioritise those cases which enable us to address the highest harm and see the greatest improvements in services. As noted above, much of our formal enforcement action in this area is subject to appeal and ongoing litigation which takes both significant resource for our office and will likely take years to resolve. We are engaging with government and other stakeholders around the possibility of reforms to the tribunal appeal process and other ways in which we can continue our collective mission of driving standards up across industry.

The proposal to amend data protection law

The consultation asks at what age a child should be able to provide their own consent to the processing of personal information by an online service under article 8 of the UK GDPR. It refers to this as the ’digital age of consent'. It also asks for views on the risks and burdens of raising the digital age of consent and what should be considered to make the proposal viable. This should not be conflated with the proposed change to the age at which children can access social media, which is a separate proposal.

In our view, there would be limited benefits to raising the age of digital consent in isolation. This is because consent is only one of the lawful bases which data controllers (in this case online services) can rely on to

use personal information. Consent is most commonly used when a data controller wishes to give users a choice over whether their data is used or when the law requires it for certain activities. It is unlikely to be an appropriate lawful basis for processing that is integral to the provision of large online services.

Raising the age of digital consent would have no effect for online services choosing to rely on one of the other lawful bases for processing, such as legitimate interests. Attempts to restrict other lawful bases that online services may use, in order to push them to rely on consent or parental consent, is also unlikely to be an effective approach. Consent is simply not an appropriate basis for many uses of personal information because of the varied approaches and contexts of processing across online services.

This would place responsibility with parents to decide whether a service could process the data of children under that age. Organisations would need to then make reasonable efforts to ensure that parents had provided consent.

As noted above, organisations that choose to set a minimum age as part of their terms of service will have no lawful basis for processing the information of children who are under that minimum age. However, raising the age of consent in data protection law will not necessarily result in organisations changing the minimum age at which children can access their services. It would not therefore constitute a ban on children accessing those services without parental consent. If government's policy aim is to prevent access to social media for children under a certain age, then raising the age of digital consent is unlikely to achieve it.

Government should also consider the broad scope of services that such a measure would impact, given that article 8 applies to information society services offered directly to children, rather than simply social media platforms. Therefore, if the policy intent is to target a narrower set of online services, it should look to identify this in any legislative changes.

The data protection implications of the wider proposals for legislative changes

Restricting access to social media services or certain functionality by age

The consultation asks whether there should be a ban on access to social media services for under 13s and asks for views on what the impact of such a ban would be. It also asks whether certain functionality should be age-restricted.

We support government taking an evidence-based approach when considering potential restrictions on children's access to functionalities. While we do not take a position on whether and where a legal minimum age should be set, we emphasise that minimum age rules alone do not eliminate the risks associated with data processing. They also don't replace the need for data protection by design and high privacy defaults.

Our Children's code says that, to meet fairness and lawfulness requirements, online services should assess the risks arising from the use of children's personal information using a data protection impact assessment and design their services to meet the standards in the Children's code to mitigate those risks. The Data (Use and Access) Act 2025 strengthened requirements in data protection law, requiring services to take into account that children merit specific protection in relation to the use of their personal information and have different needs at different ages and stages of development as they design their services.[5]

For a statutory ban or functionality restrictions to be effective, they must be accompanied by requirements for effective age assurance. Where services rely on weak age checks, a formal ban risks providing false assurance, with children continuing to access services in practice whilst platforms assume compliance. Without effective age assurance a ban will likely fail to deliver the intended benefits. We note that, currently, many platforms fail to enforce their own minimum age requirements or rely on self-declaration, which is easily circumvented.

We therefore consider that robust age assurance requirements will be central to the effectiveness of any minimum age restriction, whether that is access to a whole service or to certain functionality. We recognise that all age assurance methods involve the processing of personal information. Organisations can process personal information for age assurance, as long as the method used is necessary, proportionate to the risks and complies with data protection legislation.

[5] See Article 25 of the UK GDPR as amended by the Data Use and Access Act (2025)

The Commissioner's Opinion on age assurance for the Children's code, published before the implementation of the OSA, sets out our expectations on this topic in detail. The ICO-approved certification scheme is also a way for age assurance providers to demonstrate compliance with data protection law.

The OSA's provisions and expectations on age assurance are supported by statutory guidance from Ofcom on what constitutes highly-effective age assurance (HEAA). We provided input and data protection expertise to Ofcom during the production of its protection of children codes and HEAA guidance. This included directing service providers to our guidance to familiarise themselves with data protection legislation and how to apply it to age assurance methods. We also produced a joint statement with Ofcom on age assurance which provides further information about how to comply with age assurance requirements under both data protection law and the OSA.

In our view, if government introduces an age limit for accessing services, then it should set clear standards for age assurance that maintain regulatory coherence across both the data protection and online safety regimes. This would ensure that the expectations for relevant services are clear and avoids adding to the compliance burden for organisations. Such standards should not rely on excessive data collection or unnecessarily intrusive biometrics.

Government should consider whether further work is needed to develop and potentially mandate certification systems for age assurance providers to ensure public trust and engagement in these measures. Such a system should factor in providers' accountability and demonstrable compliance with data protection law.

There may also be some unintended consequences of introducing a social media ban or limiting access to social media for under 13s:

- Some could use minimum age rules to justify weakening privacy protections for older teens.
- Minimum age rules would also apply only to a subset of online services, but could reduce the focus across the sector on providing effective privacy protections, parental controls and support for children, parents and carers on how to safely engage in the online world. We know from our own research and work that these kinds of

tools and support remain crucial for supporting children to become empowered digital citizens.
- Children may be displaced to less regulated or offshore services if access to mainstream platforms is restricted, potentially weakening both safety and data protection outcomes.
- Children's access to beneficial and protective services (eg peer support communities) may be negatively impacted.

Further comments on the consultation

Regulatory powers

We would support the government in developing proposals that are underpinned by clear and robust regulatory powers as well as a quick and efficient court and appeals process.

Whilst data protection law provides the opportunity to take regulatory action against firms that do not comply with the UK GDPR, a key challenge is obtaining sufficient, accurate and verifiable technical information from firms. It currently takes too long to progress cases and to obtain important legal judgments that contain significant interpretive case law.

In the examples above involving TikTok, we issued an information notice in March 2025 to obtain further information on the design and operation of its recommender systems. TikTok has appealed that notice. As a result, we will have to expend resources engaging in the appeal and wait until it is heard through the UK courts and appeals process before we receive any information. This means that our investigation, and any resulting change in real world practice, may be delayed for months or even years. Similarly, the appeal against the monetary penalty issued in 2023 remains ongoing. In July 2025, the First Tier Tribunal found in our favour on the preliminary issue of whether the 'special purposes' provisions applied, but the case is now under appeal to the Upper Tribunal.

Some relatively simple changes to appeals processes, such as starting appeals of enforcement or monetary penalty notices in the Upper Tribunal, rather than the First Tier, would help to reduce the time to obtain judgments. It would mirror the approach in legal frameworks overseen by our regulatory counterparts in the DRCF. Removing the full merits basis for appeals against information and assessment notices

would also help and be a more proportionate approach. We welcome ongoing engagement with government to explore these possibilities.

Scope of services

Any definition of services subject to restrictions must be clear, future-proof and aligned with the OSA. Overly narrow definitions risk missing harmful services or driving children toward less mainstream platforms which could make the policy ineffective. Equally, overly broad definitions risk making the policy intervention less effectively targeted and increasing the regulatory burden on lower-risk services.

Consultation chapter 1 - Understanding how children use technology

The consultation asks about the benefits and harms that may arise from children's social media use and being online and asks for views on where the balance lies.

We note that views on this vary and that research into causal links between harm and online behaviours is still developing and being contested via the courts (eg the recent US cases involving Meta which have been appealed[6]). We acknowledged this when developing our Children's code. We advised platforms to take a precautionary approach and not use children's personal information in ways that had been formally identified as requiring further research or evidence to establish if they were detrimental to children's health and wellbeing. This was in addition to not using data in ways that were obviously detrimental or went against regulatory advice or government recommendations.

We also referenced the UN Convention of the Rights of the Child and explained the importance of supporting children's rights (such as the right to play, privacy and freedom of association) when designing online services.

We suggest that whatever approach government takes, it should consider how this will keep pace as relevant research and evidence develops. We also caution that full consensus on these matters is unlikely. Government should therefore prepare to encounter robust challenge and to nevertheless set clear statutory expectations for others to follow.

[6] P.F., et al. (K.G.M) v. Meta Platforms, Inc., et al,. Case No. 22STCV33140) (Cal.Super.Ct. Mar 25, 2026)

Consultation chapter 2: Interventions for safer, more positive experiences

The consultation asks for views on whether measures should be taken to impose restrictions on online services about 'addiction', compulsive design and displacement.

We support government taking an evidence-based approach to its consideration of this question.

The UK GDPR requires services to consider children's higher protection matters when implementing appropriate technical and organisational measures to safeguard children's data protection rights. Additionally, the Children's code sets out an expectation that services design online experiences with the best interests of the child in mind and ensure that data processing activities are not detrimental to children's physical or mental wellbeing.

In practice, this means not using data in ways that are obviously detrimental or go against regulatory advice or government recommendations. It also means taking a precautionary approach where a need for further research or evidence is formally indicated. Through our guidance and work on children's privacy, we have consistently highlighted the risk of manipulative design patterns that subvert children's autonomy. Many of these persuasive features depend on the use of personal information, such as behavioural tracking, real-time inference and the personalisation of services via recommender systems.

We are also currently considering the risk of wellbeing harms (including excessive or compulsive use of services) posed to children using social media in the context of our recommender systems work.

Given the technical complexity and opacity of how recommender systems work, we would support initiatives that promote greater transparency, including the government consultation trial, around the harms posed to children when recommendation algorithms process their personal information.

Consultation chapter 3 – Enforcement and compliance

The consultation asks about methods that children might use to circumvent online safety rules and how to effectively reduce such

circumvention. It asks for views on the age-gating of Virtual Private Network (VPN) access.

We are aware of ways that children might circumvent online protections through our commissioned research. For instance, Families' attitudes towards age assurance shows that parents are often willing to help children circumvent age restrictions for online services.

Children may also use VPNs to circumvent age assurance. However, VPNs also bring important privacy protections for both children and adults, including:

- protecting identity or location online;
- accessing virtual learning environments securely; and
- reducing risks associated with online tracking and profiling.

Further analysis of different types of VPN may be required. This would allow government to make an informed decision about whether to age restrict certain types of VPN, to aid clarity, certainty and effectiveness. The type of VPN under consideration are consumer VPNs, which typically allow a user to select which country they want to appear from by altering their internet protocol (IP) address. However, there are many other types of VPNs used for different reasons, particularly for providing cyber security.

Consultation chapter 4: Preparing children for a digital future

The consultation asks for views on supporting families and children with media and digital literacy and promoting high-quality content to support children's learning and development.

Our research has found three in four parents fear their child can't make safe online privacy choices and 71% of parents worry the information their child shares today could affect their future.

This is why we have launched our Switched on to Privacy campaign[7], designed to help encourage and facilitate conversations between children and parents and carers about children's privacy online.

Beyond our own work, we strongly support efforts to improve children's digital and media literacy, particularly about:

- understanding how algorithms and personalisation work;
- recognising commercial intent and identifying advertising;

[7] One click too many? 75% of parents fear their kids aren't making safe choices online | ICO

- protecting personal information;
- identifying misinformation;
- challenging manipulative or deceptive design; and
- exercising data rights.

Support should be age appropriate, accessible and delivered across schools, community settings and digital environments. Digital literacy must prepare children not only to avoid harm, but to exercise agency and understand data rights as they transition into adulthood.

Consultation chapter 5 – Supporting families

The consultation asks for views on parental controls for children of different ages.

In our view, parents and carers play an important role. However, they should not be expected to compensate for systemic design risks. Parental controls should:

- be optional, transparent and easy to configure;
- avoid intrusive monitoring or surveillance of children;
- be designed in line with fairness and data minimisation principles;
- include clear explanations about what data is collected and how it is used; and
- respect the growing autonomy of older children.

Support could also include improved guidance at point-of-device sale and standardised, accessible onboarding for families.