KPMG Law

Protecting children online: What UK Service providers need to do now



KPMG. Make the Difference.

Children's online safety is now at the forefront of the UK regulatory agenda as well as being front page news. With the Children's Safety Codes of Practice under the Online Safety Act 2023 ("UK OSA") now in force and increasing alignment with data protection and digital design obligations, organisations offering online services accessible to children face heightened compliance, governance and enforcement risks.

Why children's online protection is a board-level issue

Children are recognised in the UK law as a vulnerable group requiring enhanced protection online. Regulators now expect organisations to take a proactive, risk-based and evidence-driven approach to child safety, embedding protections by design rather than relying on reactive moderation.

Key drivers include:

- Increased regulatory scrutiny and enforcement powers under the UK OSA.
- Stronger expectations around age assurance, content moderation and recommender systems.
- Direct interaction with UK GDPR obligations, including fairness, transparency and data minimisation.
- Reputational and commercial risk arising from child safety failures.
- Increased media attention on protecting children online.

The UK Children's safety codes of practice

01 What are the children's safety codes?

- Ofcom, the UK communications regulator, has published the Children's Safety Codes of Practice for user-to-user services and search services (the "Children Codes") under the UK OSA. First published in April 2025, the Children Codes came into force on 25 July 2025 following Parliamentary approval.
- The Children Codes are statutory codes setting out recommended measures that in-scope user-to-user and search service providers can take to meet their statutory child safety duties. Ofcom will assess in-scope providers on whether they have followed the Children Codes (or adopted alternative measures) to meet their children's safety duties.
- In-scope providers are deemed compliant with children's safety duties if they follow the Children's Codes, although they may use alternative measures where these achieve the same outcomes. The Children's Codes remain the primary benchmark and clearest route to compliance.

Source:

Ofcom – Children's Safety Codes of Practice (Online Safety Act 2023).

Link:

Quick guide to Protection of Children Codes.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02 Scope of Application

The Children Codes apply to: 1) User-to-user services; and 2) Search services that are likely to be accessed by children (under 18), regardless of whether the service is explicitly targeted at children. To confirm whether this Code applies to you, see Key Terminology and Definitions for user-to-user and search services.

03 Core Recommended Measures Under the Children Codes

Depending on the provider's size and user base, the recommended measures vary for different types of harmful content. The Children Codes set out 40 measures to help service providers navigate their children's safety obligations. We list here the core recommended measures under the Children Codes.

Robust Governance and Accountability

Strong and effective governance and accountability is the foundation of children's online safety. In-scope providers should assign senior ownership with the safety duties protecting children and the reporting and complaints duties, integrate child-safety considerations into product, and ensure regular board- level reporting on risks, controls and incidents.

Maintain a clear audit trail of your methodology, design decisions, tracking evidence of new and increasing harm to children, and ongoing internal monitoring and assurance so you can evidence effectiveness to Ofcom, particularly if you depart from the measures recommended in the Children's Safety Codes.

Children's Risk Assessment

Children's Risk Assessment is one of the foremost measures to be implemented annually. The initial children's risk assessment was due by 24 July 2025, with the next assessment scheduled for completion by 24 July 2026. In-scope providers must conduct a children's risk assessment annually, assess risks by age group and category of harm and identify how children may be exposed to harmful content through service features, design and algorithms.

Age Assurance

Age assurance must be highly effective to prevent children from accessing harmful content while giving access to adults to legal content. The level of assurance should be proportionate to risk. Where a service hosts or disseminates Primary Priority Content harmful to children, highly effective measures are required to block children's access. For Priority Content harmful to children, measures should be demonstrably effective and calibrated to the service's specific risk profile.

Robust age checks are a key part of a highly effective age assurance to assess whether a user is a child. For online service providers hosting or disseminating Primary Priority Content or Priority Content, highly effective age assurance measures (content controls or access controls) must be implemented to prevent children from accessing such content. Failure to do so is likely to result in significant regulatory scrutiny.



KPMG

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



Content Moderation (search moderation)

In-scope providers must have a content moderation function to review and assess suspected harmful content to children and to enable swift action against such content. Content moderation must be tailored for different age groups, proactively detect and/or remove harmful content and establish content moderation policies setting out rules, standards and guidelines and how the policies will be implemented and enforced. Moderation teams should receive training and materials to fulfill their role in moderating content.

User reporting and complaints tool

Users (including children and parents) should be able to find easy-to-use tools to report harmful content or illegal content considering the accessibility needs of children user to report, and to provide sufficient information as to how the compliant will be handled and its indicative timeframes and outcomes. In-scope providers also should allow content appeal processes, such as those manifestly unfounded complaints.

Safer Algorithms and Recommender Systems

Safer algorithms requiring the recommender system must ensure the content algorithms are configured to filter out potential harmful content in children users' content. It also includes providing age-appropriate user support materials for children and providing information to children when they restrict content or interactions with other accounts, as well as signposting children to support when encounter harmful content.

Terms of Service

Safer algorithms requiring the recommender system must ensure the content algorithms are configured to filter out potential harmful content in children users' content. It also includes providing age-appropriate user support materials for children and providing information to children when they restrict content or interactions with other accounts, as well as signposting children to support when encounter harmful content.

User controls

Service providers should enable the option of user blocking and muting with other users. Service providers should also enable the disabling comment's function where children user wish to exercise that function.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Data protection by design for child-centred digital services

01 Children's protection and the UK GDPR

Children's online protection obligations intersect directly with UK GDPR requirements. The ICO has made clear that children merit specific protection regarding their personal data, particularly in relation to fairness and transparency, lawful bases for processing, data minimisation, purpose limitation, automated decision-making and profiling.

Key areas requiring attention include:

- **Fairness and transparency:** Organisations must provide clear age-appropriate information to children and parents about data use, risks, and rights.
- **Lawful basis for processing:** Any consent obtained must be valid and informed, and the lawful basis for processing must be appropriate.
- **Data minimisation and purpose limitation:** Only the minimum necessary personal data should be collected and used for specified purposes.
- **Automated decision-making and profiling:** Particular care is required when using children's data for these purposes due to the potential impact on their rights.

The UK GDPR requires organisations to build data protection into systems and processes from the outset, with particular attention to children's needs. Where processing may pose a high risk to children's rights, a data protection impact assessment should be conducted. Children and parents should be clearly informed about data use, risks, and safeguards, with privacy settings defaulting to the most protective option. The best interests of the child must be central to all processing, and children's views should be considered where appropriate.

Recent legislation, such as the Data Use and Access Act 2025, further stress the need for lawful and well-governed data use in child-focused services. Ongoing attention to ICO guidance and enforcement is essential for compliance and effective protection of children's data. The ICO has recently fined a UK business for failing to process children's data lawfully.

02 Age-Appropriate Design Code

The Age-Appropriate Design Code formally came into effect on 2 September 2020. This is another statutory UK code under the Data Protection Act 2018 that translates UK GDPR principles into 15 design standards for online services likely to be accessed by under 18s, requiring "privacy by default" and a DPIA focused on children's risks. Alignment between the Children's Code and the Age-Appropriate Design Code is critical for managing regulatory risk in a comprehensive manner. Organisations are expected to conform with the Age-Appropriate Design Code from 2 September 2021, following a 12- month transition period.

03 Relationship between the Children Codes and Age-Appropriate Design Code

The Children Codes and the Age-Appropriate Design Code work in tandem for the better protection of children in the online space. The Children Codes aim to ensure children are not exposed to harmful content inappropriate for their age, while the Age-Appropriate Design Code implements data protection principles to protect children's data. In-scope providers are recommended to design integrated age assurance and data protection processes to satisfy both sets of obligations.



© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Practical impact for online service providers

If your company is providing user-to-user and search services that are likely to be accessed by children in the UK, it is recommended to conduct an annual child risk assessment break down by age groups and harm categories and to create and implement highly effective age assurance measures and regularly review age assurance strategies to prevent children from accessing harmful content. Maintain up-to-date content moderation policies and operational controls. The next children risk assessment is expected to be completed by 24 July 2026 and establishing a review cadence is necessary. It is good practice to have training for teams to refresh governance to oversee child safety with clear metrics and audit trails. Additionally, you need to regularly update and adjust recommender systems to ensure that they are up to date and harmful content to children can be removed quickly. Lastly, aligning your children's protection practices with the UK GDPR and the ICO's Age-Appropriate Design Code (e.g., DPIAs for age assurance and high-risk features, data minimisation, lawful bases, vendor due diligence). Failure to do so exposes organisations to enforcement action, significant fines, reputational harm and operational disruption.



© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Key terminology and definitions

Age assurance: age verification or age estimation.

Age-Appropriate Design: Designing online services with children's best interests, developmental needs and rights as a primary consideration.

Child: Any individual under the age of 18.

Children's Risk Assessment: A structured assessment identifying how a service may expose children to harmful content and the mitigations required.

ICO: The UK's Information Commissioner's Office.

In-scope Provider: any organisation that operates a user-to-user service or a search service that has links to the UK and is likely to be accessed by children, thereby bringing it within the children's safety duties under the Online Safety Act 2023.

Illegal Content: refers to any online material that constitutes a criminal offence under UK law, including terrorism, child sexual exploitation and abuse, grooming, hate and abusive behaviour, intimate image abuse, extreme pornography, encouraging or assisting suicide, fraud, trafficking, serious violent or sexual offences, and other offences listed in the Act.

Ofcom (the Office of Communication): the independent regulatory and competition authority for the UK communication industries.

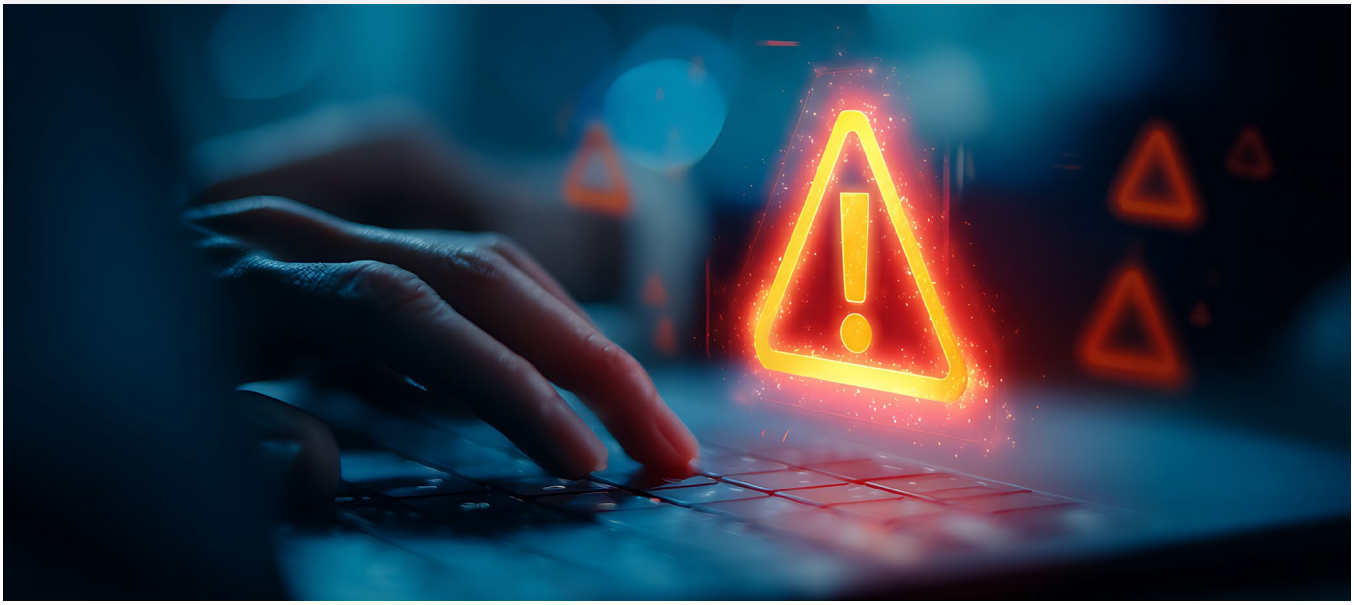
Primary Priority Content: means Primary priority content that is harmful to children under Section 61 of the Online Safety Act refers to the highest-risk categories of harmful content such as pornography, suicide content, self-harm content, and eating-disorder encouragement that platforms must strictly prevent children from accessing through robust age-assurance measures.

Priority Content: means Priority content that is harmful to children under Section 62 of the Online Safety Act refers to legally specified categories of harmful material, such as hate-targeted abuse, incitement to hatred, violent or graphic content, bullying, dangerous stunts, and encouragement of harmful substance use that pose a heightened risk to under-18s and therefore trigger the Act's strictest child-protection duties.

Search Services: An internet service that is, or includes, a search engine.

User-to-user service: an internet service by means of which content that is generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service.

User-to-user services include social media, video-sharing, user-generated pornography platforms, forums and chat rooms, marketplaces, dating services, gaming services, messaging services, file-storage and sharing platforms, information-sharing services, fundraising services, payment services, and relevant GenAI-enabled services. These service types should not be taken as a definitive view of which services or service components fall within scope of the Act.



© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

How can KPMG support?

KPMG Law UK supports organisations across the full lifecycle of data, digital and technology regulation, combining legal advice with deep regulatory and sector insight. Our lawyers work closely with KPMG's cybersecurity, privacy, risk and technology specialists to deliver integrated, pragmatic and defensible outcomes.

Our support in relation to children's online protection typically includes:

- **Conducting 'as-is' gap and readiness assessments:** Legal assessment of your current governance, policies, processes, and controls against OSA duties and relevant regulatory guidance. We identify gaps, areas of legal risk, and priority actions to support proportionate and defensible compliance planning.
- **Designing risk assessments:** Legal-led support for children's risk assessments, from scoping and harm categorisation to helping to ensure defensibility under regulatory scrutiny. This includes DPIAs for child-facing features, lawful basis and transparency assessments, data minimisation, and vendor due diligence.
- **Applying OSA duties, regulatory interpretation and horizon scanning:** Clear legal advice on the Online Safety Act 2023, Children's Safety Codes of Practice, ICO guidance and evolving regulatory expectations.
- **Introducing compliance and assurance frameworks:** Legal-led advice on the design of governance frameworks to meet statutory duties and regulatory expectations, including age assurance and access controls, content moderation and governance, and algorithmic and digital feature governance affecting children, aligned with UK GDPR and emerging AI governance standards.
- **Supporting the design of OSA, aligned policies, procedures, and processes:** Legal advice on the structure and content of policies, procedures, and internal processes relevant to individual OSA duties, aligned with applicable statutory and regulatory expectations.
- **Board, executive and regulator engagement:** Briefings, training and regulatory response support to evidence accountability, oversight and compliance by design.

Our approach is practical, risk-based and tailored to your organisation's sector, scale and digital maturity.

Looking ahead

Children's online protection will continue to evolve through regulatory guidance, enforcement activity and increased convergence with data protection and AI governance. Organisations that act early, embed compliance by design and align legal, technical and operational teams will be best placed to manage risk and build trust.

Contact us



James Cassidy
Director (Solicitor), KPMG Law
M: +44 (0)7935 351647
E: james.cassidy@kpmg.co.uk



Johanna Suárez
Manager (Solicitor), KPMG Law
M: +44 (0)7543 509767
E: johanna.suarezborja@kpmg.co.uk



Mingzhi Xie
Assistant Manager, KPMG Law
M: +44 (0)7543 509931
E: mingzhi.xie@kpmg.co.uk

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

KPMG Law is part of KPMG LLP, a multi-disciplinary practice authorised and regulated by the Solicitors Regulation Authority. SRA ID: 615423. For full details of our professional regulation please refer to 'Regulatory information' under 'About' at www.kpmg.com/uk.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity.

Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

CREATE: CRT165974A | February 2026