

















Top Tips: Kid's Privacy and Online Safety in the UK

 <p>Know your users.</p> <p>Is your service "likely to be accessed" by children (U18s)?</p> <p>On the privacy side, you have a responsibility to either (i) verify the age of your users to ensure a high-level of data protection for children specifically, or (ii) apply a "floor of protection" for all users. The level of certainty you need to have about the age of your users depends on the risks associated with your data processing.</p> <p>There are also specific children safety duties if services are likely to be accessed by children (as determined by the child accessibility assessment) under the OSA.</p>	 <p>No profiling.</p> <p>Profiling (which follows the GDPR definition), including for targeted advertising, should be off by default.</p> <p>Consider instead restricting marketing to contextual advertising that doesn't process children's data.</p>
 <p>Be transparent.</p> <p>Provide age-appropriate privacy information, in terms of both content and how it is presented. For example, use cartoons or videos and 'bite sized' explanations.</p> <p>T&Cs must also include information on how children are prevented from encountering illegal/harmful content and how they are determined to be at risk of harm.</p>	 <p>Avoid nudge techniques.</p> <p>Do not use nudge techniques to lead children to make poor privacy decisions.</p>
 <p>Make the "best interests of the child" a top priority.</p> <p>During the design and development of your service, consider how you can, for example, protect and support children's health and wellbeing, their development, and their right to freedom of association and play.</p>	 <p>Prevent the detrimental use of children's data.</p> <p>This means you should not process children's personal data in ways that are detrimental to their health and wellbeing. This ties in with the best interest standard and privacy by design principles (e.g., data minimisation, data sharing and default settings etc.)</p>
 <p>Get verifiable parental consent when you need to.</p> <p>Parental consent is only needed where you rely on consent as the legal basis for processing personal data and the child is below the age of digital consent (13 in the UK).</p>	 <p>Stop children from coming across certain content.</p> <p>Services need extra systems and processes in place to prevent children from encountering certain types of harmful or age-inappropriate content (e.g., by using age verification/estimation tools).</p> <p>Precise duties vary from service to service and type of content. There are also other measures to protect children from harm.</p>
 <p>Carry out a DPIA / child safety risk assessment.</p> <p>To identify, assess, mitigate, and manage the specific risks to children. Separately consider children in different age groups.</p>	 <p>Each online service is unique.</p> <p>Don't just copy what other services do and hope for the best. Remember, jurisdictional rules can vary too!</p>
 <p>Set high privacy settings by default.</p> <p>This means that children's personal data is only visible or shared with other users if the child allows this.</p> <p>Give age-appropriate explanations and prompts at the point children try to change any privacy settings.</p>	 <p>Age-appropriate application.</p> <p>Children in the UK means any person under 18, so don't forget that such restrictions need to apply even to older teens. Some standards, however, may vary by age.</p>
 <p>Turn geo-location tracking off by default.</p>	 <p>Online tools.</p> <p>Allow your users (including children) to report harmful content and submit complaints.</p>
 <p>Help children exercise their data protection rights.</p> <p>Make it easy and simple for them to do so. For younger children, this might need more parental involvement.</p>	 <p>Parental controls are important.</p> <p>For example, setting time limits or restricting in-app purchases. You need to make it clear to a child if controls are being used, and any controls should consider the best interests of the child standard and be balanced against the child's rights to privacy and autonomy.</p>