Age appropriate design code – Executive summary

Children are being 'datafied' with companies and organisations recording many thousands of data points about them as they grow up. These can range from details about their mood and their friendships to what time they woke up and when they went to bed.

Conforming to this statutory code of practice will ensure that as an organisation providing online services likely to be accessed by children in the UK, you take into account the best interests of the child. It will help you to develop services that recognise and cater for the fact that children warrant special protection in how their personal data is used, whilst also offering plenty of opportunity to explore and develop online.

You have 12 months to implement the necessary changes from the date that the code takes effect following the Parliamentary approval process. The ICO approach to enforcement as set out in our Regulatory Action Policy will apply. That policy and this code both apply a proportionate and risk-based approach.

The United Nations Convention on the Rights of the Child (UNCRC) recognises that children need special safeguards and care in all aspects of their life. There is agreement at international level and within the UK that much more needs to be done to create a safer online space for them to learn, explore and play.

In the UK, Parliament and government have acted to ensure that our domestic data protection laws truly transform the way we safeguard our children when they access online services by requiring the Commissioner to produce this statutory code of practice. This code seeks to protect children **within** the digital world, not protect them from it.

The code sets out 15 standards of age appropriate design reflecting a risk-based approach. The focus is on providing default settings which ensures that children have the best possible access to online services whilst minimising data collection and use, by default.

It also ensures that children who choose to change their default settings get the right information, guidance and advice before they do so, and proper protection in how their data is used afterwards.

You should follow the standards as part of your approach to complying with data protection law. If you can show us that you conform to these standards then you will conform to the code. The standards are cumulative and interlinked and you must

implement them all, to the extent they are relevant to your service, in order to demonstrate your conformity.

The detail below the standards provides further explanation to help you understand and implement them in practice. It is designed to help you if you aren't sure what to do, but it is not prescriptive. This should give you enough flexibility to develop services which conform to the standards in your own way, taking a proportionate and risk-based approach. It will help you to design services that comply with the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

Code standards

The standards are:

1. **Best interests of the child:** The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.
2. **Data protection impact assessments:** Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.
3. **Age appropriate application:** Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.
4. **Transparency:** The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.
5. **Detrimental use of data:** Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.
6. **Policies and community standards:** Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).
7. **Default settings:** Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

8. **Data minimisation:** Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.
9. **Data sharing:** Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
10. **Geolocation:** Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session.
11. **Parental controls:** If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.
12. **Profiling:** Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).
13. **Nudge techniques:** Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.
14. **Connected toys and devices:** If you provide a connected toy or device ensure you include effective tools to enable conformance to this code.
15. **Online tools:** Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.