

Age appropriate design:

a code of practice
for online services

ico.
Information Commissioner's Office



children's
code



Information Commissioner’s foreword	3
Executive summary	5
Additional resources	6
Code standards	7
About this code	9
Services covered by this code	15
Transitional arrangements	21
Standards of age appropriate design	23
1. Best interests of the child	24
2. Data protection impact assessments	27
3. Age appropriate application	32
4. Transparency	37
5. Detrimental use of data	43

Information Commissioner's foreword

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

The Secretary of State laid the Age Appropriate Design Code to Parliament under section 125(1)(b) of the Data Protection Act 2018 (the Act) on 11 June 2020. The ICO issued the code on 12 August 2020 and it will come into force on 2 September 2020 with a 12 month transition period.

There is more information in the [Explanatory Memorandum](#).

Information Commissioner's foreword

Data sits at the heart of the digital services children use every day. From the moment a young person opens an app, plays a game or loads a website, data begins to be gathered. Who's using the service? How are they using it? How frequently? Where from? On what device?

That information may then inform techniques used to persuade young people to spend more time using services, to shape the content they are encouraged to engage with, and to tailor the advertisements they see.

For all the benefits the digital economy can offer children, we are not currently creating a safe space for them to learn, explore and play.

This statutory code of practice looks to change that, not by seeking to protect children from the digital world, but by protecting them within it.

This code is necessary.

This code will lead to changes that will help empower both adults and children.

One in five UK internet users are children, but they are using an internet that was not designed for them. In our own research conducted to inform the direction of the code, we heard children describing data practices as "nosy", "rude" and a "bit freaky".

Our recent national survey into people's biggest data protection concerns ranked children's privacy second only to cyber security. This mirrors similar sentiments in research by Ofcom and the London School of Economics.

This code will lead to changes in practices that other countries are considering too.

It is rooted in the United Nations Convention on the Rights of the Child (UNCRC) that recognises the special safeguards children need in all aspects of their life. Data protection law at the European level reflects this and provides its own additional safeguards for children.

The code is the first of its kind, but it reflects the global direction of travel with similar reform being considered in the USA, Europe and globally by the Organisation for Economic Co-operation and Development (OECD).

This code will lead to changes that UK Parliament wants.

Parliament and government ensured UK data protection laws will truly transform the way we look after children online by requiring my office to introduce this statutory code of practice.

The code delivers on that mandate and requires information society services to put the best interests of the child first when they are designing and developing apps, games, connected toys and websites that are likely to be accessed by them.

This code is achievable.

The code is not a new law but it sets standards and explains how the General Data Protection Regulation applies in the context of children using digital services. It follows a thorough consultation process that included speaking with parents, children, schools, children's campaign groups, developers, tech and gaming companies and online service providers.

Such conversations helped shape our code into effective, proportionate and achievable provisions.

Organisations should conform to the code and demonstrate that their services use children's data fairly and in compliance with data protection law.

The code is a set of 15 flexible standards – they do not ban or specifically prescribe – that provides built-in protection to allow children to explore, learn and play online by ensuring that the best interests of the child are the primary consideration when designing and developing online services.

Settings must be “high privacy” by default (unless there's a compelling reason not to); only the minimum amount of personal data should be collected and retained; children's data should not usually be shared; geolocation services should be switched off by default. Nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings. The code also addresses issues of parental control and profiling.

This code will make a difference.

Developers and those in the digital sector must act. We have allowed the maximum transition period of 12 months and will continue working with the industry.

We want coders, UX designers and system engineers to engage with these standards in their day-to-day to work and we're setting up a package of support to help.

But the next step must be a period of action and preparation. I believe companies will want to conform with the standards because they will want to demonstrate their commitment to always acting in the best interests of the child. Those companies that do not make the required changes risk regulatory action.

What's more, they risk being left behind by those organisations that are keen to conform.

A generation from now, I believe we will look back and find it peculiar that online services weren't always designed with children in mind.

When my grandchildren are grown and have children of their own, the need to keep children safer online will be as second nature as the need to ensure they eat healthily, get a good education or buckle up in the back of a car.

And while our code will never replace parental control and guidance, it will help people have greater confidence that their children can safely learn, explore and play online.

There is no doubt that change is needed. The code is an important and significant part of that change.

Elizabeth Denham CBE

Executive summary

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

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).

Additional resources

Age appropriate design code

Code standards

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

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).

- .3. **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.
- .4. **Connected toys and devices:** If you provide a connected toy or device ensure you include effective tools to enable conformance to this code.
- .5. **Online tools:** Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

About this code

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

At a glance

This code explains how to ensure your online services appropriately safeguard children's personal data. You should follow the code to help you process children's data fairly. It will also enable you to design services that comply, and demonstrate you comply, with the GDPR and PECR. If you do not follow this code, you are likely to find it more difficult to demonstrate your compliance with the law, should we take regulatory action against you.

- [Who is this code for?](#)
- [What is the purpose of this code?](#)
- [What is the status of this code?](#)
- [How should we use the code?](#)

Who is this code for?

This code is for providers of information society services (ISS). It applies to you if you provide online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen) that process personal data and are likely to be accessed by children in the UK. It is not only for services aimed at children. In this code 'online service' means a relevant ISS. For more information, see the separate section on [services covered by this code](#).

What is the purpose of this code?

This code addresses how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of, children.

It reflects the increasing concern about the position of children in society and the modern digital world in particular. There is agreement at international level and within the UK that much more needs to be done to create a safe online space for them to learn, explore and play. This code achieves this not by seeking to protect children from the digital world, but by protecting them within it.

The UNCRC recognises that children need special safeguards and care in all aspects of their life and requires that these should be guaranteed by appropriate legal protections. European level data protection law reflects this and provides its own additional safeguards for children.

In the UK, Parliament and government have acted to ensure that our domestic data protection laws do 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 delivers on Parliament and the government's intent to use data protection law to make a profound and lasting change to how we look after our children when they access online services.

It takes account of the standards and principles set out in the UNCRC, and sets out specific protections for

children's personal data in compliance with the provisions of the GDPR.

If you provide relevant online services, this code will help you to comply, and demonstrate that you comply, with your data protection obligations. Conforming to the standards in this code will be a key measure of your compliance with data protection laws. Following this code will also show parents and other users of your services that you take children's privacy seriously, you can be trusted with children's data, and your services are appropriate for children to use.

How does this code take account of the rights of the child?

In preparing this code, the Commissioner is required to consider the UK's obligations under the UNCRC, and the fact that children have different needs at different ages.

The code incorporates the key principle from the UNCRC that the best interests of the child should be a primary consideration in all actions concerning children. It also aims to respect the rights and duties of parents, and the child's evolving capacity to make their own choices.

In particular, this code aims to ensure that online services use children's data in ways that support the rights of the child to:

- freedom of expression;
- freedom of thought, conscience and religion;
- freedom of association;
- privacy;
- access information from the media (with appropriate protection from information and material injurious to their well-being);
- play and engage in recreational activities appropriate to their age; and
- protection from economic, sexual or other forms of exploitation.

How does this code support parents?

Parents (or guardians) play a key role in protecting their children and deciding what is in their best interests. However, in the context of online services, parents and children may find it difficult to make informed choices or exercise any control over the way those services use children's data. Often the only choice in practice is to avoid online services altogether, which means the child loses the benefits of online play, interaction and development. This code therefore expects providers of these services to take responsibility for ensuring that the way their services use personal data is appropriate to the child's age, takes account of their best interests, and respects their rights; as well as supporting parents or older children in making choices (where appropriate) in the child's best interests.

How does this code support data protection compliance?

The UK data protection regime is set out in the Data Protection Act 2018 (DPA 2018) and the GDPR. This regime requires you to take a risk-based approach when you use people's data, based on certain key principles, rights and obligations.

This code supports compliance with those general principles by setting out specific protections you need to build in when designing online services likely to be accessed by children, in line with Recital 38 of the GDPR:



“Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child...”

In particular, this code sets out practical measures and safeguards to ensure processing under the GDPR can be considered ‘fair’ in the context of online risks to children, and will help you comply with:

- Article 5(1)(a): the fairness, lawfulness and transparency principle;
- Article 5(1)(b): the purpose limitation principle;
- Article 5(1)(c): the data minimisation principle;
- Article 5(1)(e): the storage limitation principle;
- Article 5(2): the accountability principle;
- Article 6: lawfulness of processing;
- Articles 12, 13 and 14: the right to be informed;
- Articles 15 to 20: the rights of data subjects;
- Article 22: profiling and automated decision-making;
- Article 25: data protection by design and by default; and
- Article 35: data protection impact assessments (DPIAs).

It covers your use of ‘inferred data’ (information about a child that you don’t collect directly, but that you infer from other information or from their behaviours online) as well as data you collect directly from the child.

Annex C also includes some guidance on identifying your lawful basis for processing in the context of an online service. If you rely on consent, it explains the Article 8 rule on parental consent for children under 13.

PECR also set some specific rules on the use of cookies and other technologies which rely on access to user devices, and on electronic marketing messages. This code refers to those requirements where relevant, but for full details on how to comply you should read our separate [Guide to PECR](#).

If you need to process personal data in order to protect children from online harms, such as child sexual exploitation and abuse, then this code shouldn’t prevent you from doing so. However, you need to satisfy all the usual data protection requirements before you proceed, such as ensuring that the processing is fair and proportionate to the harm you are seeking to prevent, identifying a lawful basis for processing and providing transparency information.

What is the status of this code?

What is the legal status of the code?

This is a statutory code of practice prepared under section 123 of the DPA 2018:



“The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age appropriate design of relevant information society services which are likely to be accessed by children.”

It was laid before Parliament on 11 June 2020 and issued on 12 August 2020 under section 125 of the DPA 2018. It comes into force on 2 September 2020.

As was made clear in the Parliamentary debates when the Data Protection Bill passed through Parliament, if your online service fails to conform to a provision of this code you may find it difficult to demonstrate compliance with the law and you may invite regulatory action.

In accordance with section 127 of the DPA 2018, the Commissioner must take the code into account when considering whether an online service has complied with its data protection obligations under the GDPR or PECR. In particular, the Commissioner will take the code into account when considering questions of fairness, lawfulness, transparency and accountability under the GDPR, and in the use of her [enforcement powers](#).

The code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant.

What happens if we don't conform to the standards in this code?

If you don't conform to the standards in this code, you are likely to find it more difficult to demonstrate that your processing is fair and complies with the GDPR and PECR. If you process a child's personal data in breach of the GDPR or PECR, we can take action against you.

Tools at our disposal include assessment notices, warnings, reprimands, enforcement notices and penalty notices (administrative fines). For serious breaches of the data protection principles, we have the power to issue fines of up to €20 million (£17.5 million when the UK GDPR comes into effect) or 4% of your annual worldwide turnover, whichever is higher.

Our approach to using these powers will take account of the risks to children that arise from your data processing, and the efforts you have made to conform to the standards in this code. In cases where we find against you, we are more likely to allow you time to bring your service into compliance if you have a well-documented and reasoned case to support the approach you have taken.

Conversely, if you have not taken proper steps to conform despite clear evidence or constructive knowledge that children are likely to access your service, and clear evidence of significant risk arising from the use of children's data, we are more likely to take formal regulatory action. The established ICO approach to enforcement as set out in our [Regulatory Action Policy](#) will apply to use of children's personal data under the GDPR and consideration of this code.

For more information, see the separate section on [enforcement of this code](#).

How is this code affected when the UK leaves the EU?

This code is based on and refers to the relevant provisions of the DPA 2018 and GDPR as they apply in the UK in November 2019, before exit day.

If the UK leaves the EU with no deal, the EU version of the GDPR will no longer be law in the UK. However, a UK version of the GDPR will be written into UK law (UK GDPR). The UK GDPR will sit alongside an amended version of the DPA 2018. Although this code is based on the provisions of the DPA 2018 and EU GDPR in effect before exit day, the key data protection principles, rights and obligations underlying this code will remain the same under the UK GDPR.

The standards in this code will therefore still apply. The Commissioner will continue to take the code into account. However, after exit day, you should read references in this code to the GDPR as references to the equivalent provision in the UK GDPR. We have also highlighted a few specific changes throughout this code where directly relevant.

If the UK agrees to leave the EU with a deal, there will be an implementation period during which the GDPR – and this code – will continue to apply in the UK in the same way as before exit day. At the end of the implementation period, the default position is the same as for a no-deal exit, and we expect this code to remain in effect.

If there are any further changes to the details of the future UK regime, the Commissioner will review the standards in this code to ensure they remain relevant and appropriate to support compliance with UK law.

What is the status of 'further reading' or other linked resources?

Any further reading or other resources which are mentioned in or linked from this code do not form part of the code. We provide links to give you helpful context and further guidance on specific issues, but there is no statutory obligation under the DPA 2018 for the Commissioner or courts to take it into account (unless it is another separate statutory code of practice).

Where we link to other ICO guidance, that guidance will inevitably reflect the Commissioner's views and inform our general approach to interpretation, compliance and enforcement.

We may also link to relevant guidance provided by the European Data Protection Board (EDPB), which is the independent body established to ensure consistency within the EU when interpreting the GDPR and taking regulatory action.

How should we use the code?

The [standards at the start of this code](#) are the 15 headline 'standards of age appropriate design' that you need to implement. The main body of this code is then divided into 15 sections, each giving more detail on what the standard means, why it is important, and how you can implement it. This further explanation is designed to help you if you aren't sure what to do, but it is not prescriptive. It 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 GDPR and PECR.

Your conformity to the code will be assessed against the 15 headline standards. However, we recommend that you read the code in full as it will help you understand how you can implement each standard properly. These standards are cumulative and interdependent - you must implement all of them, to the extent they are relevant to your service, in order to demonstrate your conformance to the code.

This code assumes familiarity with key data protection terms and concepts. We have included a glossary at the end of this code as a quick reference point for common concepts and abbreviations, but if you need an introduction to data protection – or more context and guidance on key concepts – you should refer to our separate [Guide to Data Protection](#).


This code focuses on specific safeguards to ensure your data regime is appropriate for children who are

likely to access your service, so that you process their data fairly. It is not intended as an exhaustive guide to data protection compliance. For example, it does not elaborate on your obligations on security, processors or breach reporting. You need to make sure you are aware of all of your obligations, and you should read this code alongside our other guidance. Your DPIA process should incorporate measures to comply with your data protection obligations generally, as well as conform to the specific standards in this code.

Further reading outside this code

[United Nations Convention on the Rights of the Child](#) 

[Guide to Data Protection](#) 

[Guide to PECR](#) 

[ICO Regulatory Action Policy](#) 

[DP and Brexit](#) 

Services covered by this code

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

At a glance

This code applies to “information society services likely to be accessed by children” in the UK. This includes many apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. It is not restricted to services specifically directed at children.

In more detail

- [What services does this code apply to?](#)
- [What do you mean by an 'information society service'?](#)
- [What types of online services are not 'relevant ISS'?](#)
- [When are services 'likely to be accessed by children'?](#)
- [Does it apply to services based outside the UK?](#)
- [What about the eCommerce Regulations 2002?](#)

What services does this code apply to?

Section 123 of the DPA 2018 says that this code applies to:



“relevant information society services which are likely to be accessed by children.”

It says that ‘information society services’ has the same meaning as it has in the GDPR except that it does not include ‘preventive or counselling services’, and that ‘relevant ISS’ are those which involve the processing of personal data to which the GDPR applies.

The vast majority of online services used by children are covered, although there are some limited exceptions that are discussed in more detail below. Annex A to this code provides a flowchart setting out the questions you will need to answer if you are uncertain whether your service is covered.

What do you mean by an ‘information society service’?

The definition is broad and the majority of online services that children use are covered.

‘Information society service’ is defined as:



"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:



- (i) 'at a distance' means that the service is provided without the parties being simultaneously present;
- (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."

Essentially this means that most online services are ISS, including apps, programs and many websites including search engines, social media platforms, online messaging or internet based voice telephony services, online marketplaces, content streaming services (eg video, music or gaming services), online games, news or educational websites, and any websites offering other goods or services to users over the internet. Electronic services for controlling connected toys and other connected devices are also ISS.

These services are covered even if the 'remuneration' or funding of the service doesn't come directly from the end user. For example, an online gaming app or search engine that is provided free to the end user but funded via advertising still comes within the definition of an ISS. This code also covers not-for-profit apps, games and educational sites, as long as those services can be considered as 'economic activity' in a more general sense. For example, they are types of services which are typically provided on a commercial basis.

If you are a small business with a website, your website is an ISS if you sell your products online, or offer a type of service which is transacted solely or mainly via your website without you needing to spend time with the customer in person.

What types of online services are not 'relevant ISS'?

Some services provided by public authorities

If you are a public authority which provides an online public service then, as long as the type of service you offer is not typically provided on a commercial basis your service is not a relevant ISS. This is because it is not a service 'normally provided for remuneration'.

If you are a police force or other competent authority with an online service which processes personal data for law enforcement purposes, then your service isn't a relevant ISS. This is because relevant ISS are those which involve the processing of personal data 'to which the GDPR applies'. The GDPR does not apply to processing by competent law enforcement authorities for law enforcement purposes. For further information about the scope of the GDPR and how data protection law applies to processing for law

enforcement purposes see our [Guide to data protection](#).

Websites which just provide information about a real-world business or service

If your website just provides information about your real-world business, but does not allow customers to buy products online or access a specific online service, it is not an ISS. This is because the service being offered is not provided 'at a distance'. An online booking service for an in-person appointment does not qualify as an ISS.

Traditional voice telephony services

Traditional voice telephony services are not relevant ISS. This is because they are not considered to be 'delivered by electronic means'. This differs from internet based voice calling services (VOIP) which are within scope as they are delivered over the internet by electronic means.

General broadcast services

The definition of an ISS does not include broadcast services such as scheduled television or radio transmissions that are broadcast to a general audience, rather than at the request of the individual (even if the channel is broadcast over the internet).

This differs from 'on demand' services which are, by their nature, provided 'at the individual request of a recipient'.

If you provide both a general broadcast and an on demand service, then the on demand element of your service will be covered by the code.

Preventive or counselling services

This code does not apply to websites or apps specifically offering online counselling or other preventive services (such as health screenings or check-ups) to children. This is because s123 scopes out 'preventive or counselling services'. However, more general health, fitness or wellbeing apps or services are covered.

When are services 'likely to be accessed by children'?

This code applies if children are likely to use your service. A child is defined in the UNCRC and for the purposes of this code as a person under 18.

If your service is designed for and aimed specifically at under-18s then the code applies. However, the provision in section 123 of the DPA is wider than this. It also applies to services that aren't specifically aimed or targeted at children, but are nonetheless likely to be used by under-18s.

It is important to recognise that Parliament sought to use the wording 'likely to be accessed by' rather than narrower terms, to ensure that the application of the code did not exclude services that children were using in reality. This drew on experience of other online child protection regimes internationally, that only focused on services designed for children and therefore left a gap in coverage and greater risk.

We consider that for a service to be 'likely' to be accessed, the possibility of this happening needs to be more probable than not. This recognises the intention of Parliament to cover services that children use in reality, but does not extend the definition to cover all services that children could possibly access.

In practice, whether your service is likely to be accessed by children or not is likely to depend on:

- the nature and content of the service and whether that has particular appeal for children; and

- the way in which the service is accessed and any measures you put in place to prevent children gaining access.

You should take a common sense approach to this question. If your service is the kind of service that you would not want children to use in any case, then your focus should be on how you prevent access (in which case this code does not apply), rather than on making it child-friendly. For example, if it is an adult only, restricted, or otherwise child-inappropriate service. This code should not lead to the perverse outcome of providers of restricted services having to make their services child-friendly.

If your service is not aimed at children but is not inappropriate for them to use either, then your focus should be on assessing how appealing your service will be to them. If the nature, content or presentation of your service makes you think that children will want to use it, then you should conform to the standards in this code.

If you have an existing service and children form a substantive and identifiable user group, the 'likely to be accessed by' definition will apply.

Given the breadth of application, the ICO recognises that it will be possible to conform to this code in a risk-based and proportionate manner.

If you decide that your service is not likely to be accessed by children and that you are therefore not going to implement the code then you should document and support your reasons for your decision. You may wish to refer to market research, current evidence on user behaviour, the user base of similar or existing services and service types and testing of access restriction measures.

If you initially judge that the service is not likely to be accessed by children, but evidence later emerges that a significant number of children are in fact accessing your service, you will need to conform to the standards in this code or review your access restrictions if you do not think it is appropriate for children to use your service.

Does it apply to services based outside the UK?

This code is issued under the DPA 2018. The DPA 2018 applies to online services based in the UK.

It also applies to online services based outside the UK that have a branch, office or other 'establishment' in the UK, and process personal data in the context of the activities of that establishment.

The DPA 2018 may also apply to some other services based outside the UK even if they don't have an establishment in the UK. If the relevant establishment is outside the European Economic Area (EEA), the DPA 2018 still applies if you offer your service to users in the UK, or monitor the behaviour of users in the UK. The code applies if that service is likely to be accessed by children.

If you don't have a UK establishment, but do have an establishment elsewhere in the EEA this code does not apply (even if you offer your service to UK users, or monitor the behaviour of users in the UK).

If the code applies to your processing but, under the GDPR 'one-stop-shop' arrangements you have a lead supervisory authority other than the ICO, then we may ask them to take the code into account when considering your compliance with the GDPR and PECR. Alternatively, if we consider the case to be a 'local' case (affecting UK users only), we may take action ourselves and take the code into account.

How will this change when the UK leaves the EU?

When the UK leaves the EU (or at the end of the implementation period, if the UK leaves the EU with a

deal), the UK regime will apply to services established in the EEA who are targeting UK users in the same way as to services established outside the EEA. The UK will no longer be part of the GDPR one-stop-shop system.

If you are established in the EEA and offer your service to UK users, or monitor the behaviour of users in the UK, this code will apply to you from exit day (or from the end of the implementation period if a deal is agreed).

What about the eCommerce Regulations 2002?

The eCommerce Regulations 2002 (ECR) do not exempt you from compliance with your data protection obligations. Regulation 3(1)(b) of the ECR, as amended by Schedule 19 Part 2 paragraph 288 of the DPA 2018, states that:



'Nothing in these Regulations shall apply in respect of –

(b) questions relating to information society services covered by the GDPR and Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)'

Whilst the ECR includes a 'safe harbour' regime for certain activities that you may carry out as an 'intermediary' service provider, it is important to note that:

- this does not remove your responsibility for data protection compliance, either in general or in relation to those activities; and
- the provisions of the GDPR are without prejudice to this regime.

The ICO will take the safe harbour regime into account, particularly in cases of complaints and potential regulatory action arising from activities relating to those that the safe harbour regime covers.

You should assess how the legal framework applies to activities you perform in your own right, and those which you perform as an intermediary. For example, an Internet Service Provider (ISP) or Mobile Network Operator (MNO) might provide core connectivity services as an intermediary service provider whilst also providing services such as customer service Apps or corporate websites in their own right. If necessary you may need to obtain specialist legal advice.

For more information, see the section on 'Enforcement of this Code'.

Further reading outside this code

For further information on the definition of an ISS see:

[Article 1\(1\) and Annex 1 of Directive \(EU\) 2015/1535 \(Article 4\(25\) of the GDPR incorporates this definition into the GDPR\)](#) [Ker-Optika v ANT SZ \(CJEU case C-108/09, 2 December 2010\)](#) [McFadden v Sony \(CJEU case C-484/14, 15 September 2016\)](#) [Elite Taxi v Uber \(Opinion of the AG in case C-434/15, 11 May 2017\)](#)

For more information on whether the GDPR applies, see our guidance:

[Introduction to Data Protection - Which regime? !\[\]\(77be28c87e114c3a7366fe2e09e28233_img.jpg\)](#)

For more information on the GDPR one-stop-shop principle, see the [EDPB guidelines on the lead supervisory authority !\[\]\(76571bca9499390beeae0a355d0e74a9_img.jpg\)](#).

The ICO has launched [a consultation on a package of support](#) for the providers of online services likely to be accessed by children.

Transitional arrangements

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

At a glance

Providers of ISS likely to be accessed by children should bring their processing in line with the standards in this code by 2 September 2021.

In more detail

- [When will the code take effect?](#)
- [What should we do about our existing services?](#)

When will the code take effect?

The code was issued on 12 August 2020.

It comes into force on 2 September 2020.

From 2 September 2021 the Commissioner must take the code into account when considering whether an online service has complied with its data protection obligations under the GDPR and PECR. The courts must also take the provision of the code into account, when relevant, from this date.

Our approach is to encourage conformance and we would encourage you to start preparing for the code taking effect sooner rather than later. In accordance with our Regulatory Action Policy, when considering any enforcement action we will take into account the efforts you have made towards conformance during the transition period, as well as the size and resources of your organisation, and the risks to children inherent in your data processing.

The code will apply to both new and existing services.

What should we do about our existing services?

We recommend that you start by reviewing your existing services to establish whether they are covered.

For services that are covered, you should already have a DPIA – but you should now review it (or conduct a new one) as soon as possible. This will give you the maximum amount of time available to you to bring your processing into line with the standards in the code. You should focus on assessing conformance with the standards in this code and identifying any additional measures necessary to conform.

You should make changes to your service as soon as possible, and in any event by 2 September 2021.

Where changes include changes to physical rather than purely online products, then you should ensure that the necessary changes are incorporated into manufacturing cycles schedules commencing after 2 September 2021. For example, if you are making changes to packaging, printed information or the physical component of a connected toy or device. You will not be required to recall or amend existing stock, or to

amend manufacturing cycles that were already scheduled to commence before 2 September 2021 when this code came into force.

You should also consider how to manage any changes to the way in which your service operates with your existing users. You should think about how their online experience might change and how best to communicate and prepare them for these changes so that any impact is properly managed.

Standards of age appropriate design

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

Section 123 of the DPA 2018 says this code must contain:

“

“such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children.”

It defines ‘standards of age-appropriate design’ as:

“

“such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children.”

The standards are not intended as technical standards, but as a set of technology-neutral design principles and practical privacy features. The focus of the code is to set a benchmark for the appropriate protection of children’s personal data. Different services will require different technical solutions.

You must build the standards set out in this code into your design processes from the start, into subsequent upgrade and service development processes and into your DPIA process.

For more information on how we enforce these standards, see the separate section on [enforcement of this code](#).

1. Best interests of the child

**This code came into force on 2 September 2020, with a 12 month transition period.
Organisations should conform by 2 September 2021.**

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.

What do you mean by ‘the best interests of the child’?

The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child (UNCRC):



“In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.”

The UNCRC incorporates provisions aimed at supporting the child’s needs for safety, health, wellbeing, family relationships, physical, psychological and emotional development, identity, freedom of expression, privacy and agency to form their own views and have them heard. Put simply, the best interests of the child are whatever is best for that individual child.

The UNCRC expressly recognises the role of parents and carers (including extended family, guardians and others with legal responsibility) in protecting and promoting the best interests of the child.

It also recognises the child’s right to privacy and freedom from economic exploitation. The importance of access to information, association with others, and play in supporting the child’s development. And the child’s right, in line with their evolving capacities, to have a voice in matters that affect them.

The UNCRC provides a framework which balances a number of different interests and concerns, with the intention of providing whatever is best for each individual child.

The placing of the best interests of the child as a ‘primary consideration’ recognises that the best interests of the child have to be balanced against other interests. For example the best interests of two individual children might be in conflict, or acting solely in the best interests of one child might prejudice the rights of others. It is unlikely however that the commercial interests of an organisation will outweigh a child’s right to privacy.

Why is this important?

This is important because the Information Commissioner is required to have regard to the United Kingdom’s obligations under the UNCRC in drafting this code.

It is also important because it provides a framework to help you understand the needs of children and the

rights that you have to take into account when designing online services.

Article 5(1)(a) of the GDPR says personal data shall be:



“processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)”

And recital 38 to the GDPR says:



“Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing...”

If you consider the best interests of child users in all aspects of your design of online services, then you should be well placed to comply with the ‘lawfulness, fairness and transparency’ principle, and to take proper account of Recital 38.

The principle of ‘the best interests of the child’ is therefore both something that you specifically need to consider when designing your online service, and a theme that runs throughout the provisions of this code.

How can we make sure that we meet this standard?

Consider and support the rights of children

In order to implement this standard you need to consider the needs of child users and work out how you can best support those needs in the design of your online service, when you process their personal data. In doing this you should take into account the age of the user. You may need to use evidence and advice from expert third parties to help you do this.

In particular you should consider how, in your use of personal data, you can:

- keep them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;
- protect and support their health and wellbeing;
- protect and support their physical, psychological and emotional development;
- protect and support their need to develop their own views and identity;
- protect and support their right to freedom of association and play;
- support the needs of children with disabilities in line with your obligations under the relevant equality legislation for England, Scotland, Wales and Northern Ireland;
- recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and
- recognise the evolving capacity of the child to form their own view, and give due weight to that view.

Taking account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests. Your commercial interests may not be incompatible with the best interests of the child, but you need to account for the best interests of the child as a primary consideration where any conflict arises.

Further reading outside this code

[United Nations Convention of Rights of the Child](#) 

2. Data protection impact assessments

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

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.

What do you mean by a ‘DPIA’?


A DPIA is a defined process to help you identify and minimise the data protection risks of your service – and in particular the specific risks to children who are likely to access your service which arise from your processing of their personal data.

You should begin a DPIA early in the design of your service, before you start your processing. It should include these steps:

- Step 1: identify the need for a DPIA
- Step 2: describe the processing
- Step 3: consider consultation
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks arising from your processing
- Step 6: identify measures to mitigate the risks
- Step 7: sign off, record and integrate outcomes

The DPIA process is designed to be flexible and scalable. You can design a process that fits with your existing approach to design and development, as long as it contains these key elements, and the outcomes influence the design of your service. It does not need to be a time-consuming process in every case.

Further reading outside this code

See our [detailed guidance on DPIAs](#) 

Why are DPIAs important?

DPIAs are a key part of your accountability obligations under the GDPR, and help you adopt a ‘data protection by design’ approach. A good DPIA is also an effective way to assess and document your compliance with all of your data protection obligations and the provisions of this code.

The GDPR says you must do a DPIA before you begin any **type of processing** that is **likely to result in a high risk** to the rights and freedoms of individuals.

This is not about whether your service is actually high risk, but about screening for potential indicators of

high risk. The nature and context of online services within the scope of this code mean they inevitably involve a type of processing likely to result in a high risk to the rights and freedoms of children.

The ICO is required by Article 35(4) of the GDPR to publish a list of processing operations that require a DPIA. This list supplements GDPR criteria and relevant European guidelines, and includes:

“

“the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.”

Online services may also trigger several other criteria indicating the need for a DPIA, including innovative technology, large-scale profiling, biometric data, and online tracking. In practice, this means that if you offer an online service likely to be accessed by children, you must do a DPIA.

However, DPIAs are not just a compliance exercise. Your DPIA should consider compliance risks, but also broader risks to the rights and freedoms of children that might arise from your processing, including the potential for any significant material, physical, psychological or social harm.

An effective DPIA allows you to identify and fix problems at an early stage, designing data protection in from the start. This can bring cost savings and broader benefits for both children and your organisation. It can reassure parents that you protect their children’s interests and your service is appropriate for children to use. The consultation phase of a DPIA can also give children and parents the chance to have a say in how their data is used, help you build trust, and improve your understanding of child-specific needs, concerns and expectations. It may also help you avoid reputational damage later on.

How can we make sure that we meet this standard?

There is no definitive DPIA template, but you can use or adapt the [template included as an annex to this code](#) if you wish.

You must consult your Data Protection Officer (DPO) (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.

Your DPIA must have a particular focus on the specific rights of and risks to children using your service that arise from your data processing. It should also assess and document your compliance with this code. You should build these additional elements into each stage of your DPIA, not bolt them on the end.

You need to follow the usual DPIA process set out in our [separate guidance on how to conduct a DPIA](#), but you should build in the following specific issues at each stage.

Step 1: Identify when to do your DPIA

You must embed a DPIA into the design of any new online service that is likely to be accessed by children. You must complete your DPIA before the service is launched, and ensure the outcomes can influence your design. You should not treat a DPIA as a rubber stamp or tick-box exercise at the end of the design process.

You must also do a DPIA if you are planning to make any significant changes to the processing operations

of an existing online service likely to be accessed by children.

An external change to the wider context of your service may also prompt you to review your DPIA. For example, if a new security flaw is identified, or a new public concern is raised over specific features of your service or particular risks to children.

Further reading outside this code

[ICO list of processing operations that require a DPIA](#) 

[European guidelines on DPIAs](#) 

Step 2: Describe the processing

You need to describe the nature, scope, context and purposes of the processing. In particular, you should include:

- whether you are designing your service for children;
- if not, whether children are nevertheless likely to access your service;
- the age range of those children;
- your plans, if any, for parental controls;
- your plans, if any, for establishing the age of your individual users;
- the intended benefits for children;
- the commercial interests (of yourself or third parties) that you have taken into account
- any profiling or automated decision-making involved;
- any geolocation elements;
- the use of any nudge techniques;
- any processing of special category data;
- any processing of inferred data;
- any current issues of public concern over online risks to children;
- any relevant industry standards or codes of practice;
- your responsibilities under the applicable equality legislation for England, Scotland, Wales and Northern Ireland; and
- any relevant guidance or research on the development needs, wellbeing or capacity of children in the relevant age range.

Step 3: Consult with children and parents

Depending on the size of your organisation, resources and the risks you have identified, you can seek and document the views of children and parents (or their representatives), and take them into account in your design.

We will expect larger organisations to do some form of consultation in most cases. For example, you could choose to get feedback from existing users, carry out a general public consultation, conduct market research, conduct user testing, or contact relevant children's rights groups for their views. This should

include feedback on the child's ability to understand the ways you use their data and the information you provide. If you consider that it is not possible to do any form of consultation, or it is unnecessary or wholly disproportionate, you should record that decision in your DPIA, and be prepared to justify it to us. However, it is usually possible to carry out some form of market research or user feedback.

You should also consider seeking independent advice from experts in children's rights and developmental needs as part of this stage. This is especially important for services which:

- are specifically designed for children;
- are designed for general use but known to be widely used by children (such as games or social media sites); or
- use children's data in novel or unanticipated ways.

Step 4: Assess necessity, proportionality and compliance

You need to explain why your processing is necessary and proportionate for your service. You must also include information about how you comply with the GDPR, including:

- your lawful basis for processing (see Annex C);
- your condition for processing any special category data;
- measures to ensure accuracy, avoid bias and explain use of AI; and
- specific details of your technological security measures (eg hashing or encryption standards).

In addition, at this stage you should include an explanation of how you conform to each of the standards set out in this code.

Step 5: Identify and assess risks

You must consider the potential impact on children and any harm or damage your data processing may cause – whether physical, emotional, developmental or material. You should also specifically look at whether the processing could cause, permit or contribute to the risk of:

- physical harm;
- online grooming or other sexual exploitation;
- social anxiety, self-esteem issues, bullying or peer pressure;
- access to harmful or inappropriate content;
- misinformation or undue restriction on information;
- encouraging excessive risk-taking or unhealthy behaviour;
- undermining parental authority or responsibility;
- loss of autonomy or rights (including control over data);
- compulsive use or attention deficit disorders;
- excessive screen time;
- interrupted or inadequate sleep patterns;
- economic exploitation or unfair commercial pressure; or
- any other significant economic, social or developmental disadvantage.

You should bear in mind children's needs and maturity will differ according to their age and development

stage. Annex B should help you to consider this.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on children. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. You should bear in mind that some children will be less resilient than others, so you should always take a precautionary approach to assessing the potential severity of harm. You may find that there is a high risk for some age ranges, even if the risk for other age ranges is lower.

Step 6: Identify measures to mitigate those risks

You must consider whether you could make any changes to your service to reduce or avoid each of the risks you have identified. As a minimum, you should implement the measures set out in this code, but you should also consider whether you can put any additional safeguards in place as part of your service design.

Transparency is important. However, you should also identify and consider measures that do not rely on children's ability or willingness to engage with your privacy information.

Step 7: Record the conclusion

If you have a DPO, you must record their independent advice on the outcome of the DPIA before making any final decisions.

You should record any additional measures you plan to take, and integrate them into the design of your service. If you identify a high risk that you are not mitigating, you must consult the ICO before you can go ahead.

It is good practice to publish your DPIA.

Further reading outside this code

See our [detailed guidance on DPIAs](#) 

3. Age appropriate application

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

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.

What do you mean by ‘age appropriate application’?

This means that the age range of your audience and the different needs of children at different ages and stages of development should be at the heart of how you design your service and apply this code.

It also means you must apply this code so that all children are given an appropriate level of protection in how their personal data is used. There is flexibility for you to decide how to apply this standard in the context and circumstances of your online service. It will usually mean establishing (with a level of certainty that is appropriate to the risks to the rights and freedoms that arise from your data processing) what age range your individual users fall into, so that you can tailor the protections and safeguards you give to their personal data accordingly, by applying the standards in this code. You should use your DPIA to help you assess this.

Alternatively, if you can’t or don’t wish to do this, you could choose to apply the standards to all your users instead. This is so that children are afforded some protection against the risks that arise from how their personal data is used, even if you aren’t sufficiently certain whether they are children or not.

Why is this important?

The ultimate aim of this code is to ensure that online services likely to be accessed by children are appropriate for their use and meet their development needs.

Understanding the age range of children likely to access the service – and the different needs of children at different ages and stages of development – is fundamental to the whole concept of ‘age-appropriate design’.

Children are individuals, and age ranges are not a perfect guide to the interests, needs and evolving capacity of each child. However, to help you assess what is appropriate for children broadly of that age, you can use age ranges as a guide to the capacity, skills and behaviours a child might be expected to display at each stage of their development. For the purposes of this code, we have used the following age ranges and developmental stages as a guide:

- 0 - 5: pre-literate and early literacy
- 6 - 9: core primary school years
- 10-12: transition years
- 13-15: early teens

- 16-17: approaching adulthood

There is no requirement for you to design services for development stages that aren't likely to access your service, or to use these exact age ranges if you can justify why slightly different age groupings are more appropriate for your particular service.

Further information about relevant capacities, needs, skills and behaviours at each stage is set out at Annex B of this code for reference purposes, and where relevant throughout these standards.

You should also consider the needs of disabled children in line with any obligations you may have under the relevant equality legislation for England, Scotland, Wales and Northern Ireland.

The GDPR and DPA 2018 also specify that if you rely on consent for any aspects of your online service, you need to get parental authorisation for children under 13. If you do rely on consent as your lawful basis for processing personal data then these provisions have significant practical implications for you. Meeting the standards in this code should allow you to comply with these GDPR requirements in a proportionate way. See Annex C for full details.

How can we make sure that we meet this standard?

Consider the risks to children that arise from your data processing, and the level of certainty you have that you know the age of your users

You can implement this standard by following these steps:

- Think about the risks to children that would arise from your processing of their personal data. Your DPIA will help you to do this. You may wish to take into account factors such as: the types of data collected; the volume of data; the intrusiveness of any profiling; whether decision making or other actions follow from profiling; and whether the data is being shared with third parties. Both the ICO and the European Data Protection Board have also provided guidance on DPIAs which consider assessing risk in more detail.
- Consider how well you know your users. How certain are you that an individual user is an adult or a child? How confident are you about the age range your individual child users fall into.
- Decide whether the level of certainty you have about the age of your individual users is appropriate to the risks that arise from your data processing.
- If it is, then you can apply the rest of the standards in this code to your child users only.
- If it isn't, then decide whether you prefer to:
 - reduce the data risks inherent in your service;
 - put additional measures in place to increase your level of age confidence; or
 - apply the standards in this code to all users of your service (regardless of whether they have self-declared as an adult or a child).

How can we establish age with an appropriate level of certainty?

This code is not prescriptive about exactly what methods you should use to establish age, or what level of certainty different methods provide. This is because this will vary depending on the specifics of the techniques you use. We want to allow enough flexibility for you to use measures that suit the specifics of your individual service and that can develop over time. However you should always use a method that is appropriate to the risks that arise from your data processing.

Some of the methods you may wish to consider are listed below. This list is not exhaustive. Other measures may exist or emerge over time. In assessing whether you have chosen an appropriate method, we will take into account the products currently available in the marketplace, particularly for small businesses which don't have the resources to develop their own solutions.

- **Self-declaration** – This is where a user simply states their age but does not provide any evidence to confirm it. It may be suitable for low risk processing or when used in conjunction with other techniques. Even if you prefer to apply the standards in the code to all your users, self-declaration of age can provide a useful starting point when providing privacy information and age appropriate explanations of processing (see 'What does applying the standards to all users mean in practice?' for more detail).
- **Artificial intelligence** – It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with your service. Similarly you could use this type of profiling to check that the way a user interacts with your service is consistent with their self-declared age. This technique will typically provide a greater level of certainty about the age of users with increased use of your service. If you choose to use this technique then you need to:
 - tell users that you are going to do this upfront;
 - only collect the minimum amount of personal data that you need for this purpose; and
 - don't use any personal data you collect for this purpose for other purposes.
- **Third party age verification services** – You may choose to use a third party service to provide you with an assurance of the age of your users. Such services typically work on an 'attribute' system where you request confirmation of a particular user attribute (in this case age or age range) and the service provides you with a 'yes' or 'no' answer. This method reduces the amount of personal data you need to collect yourself and may allow you to take advantage of technological expertise and latest developments in the field. If you use a third party service you will need to carry out some due diligence checks to satisfy yourself that the level of certainty with which it confirms age is sufficient (PAS standard 1296 'Online age checking' may help you with this), and that it is compliant with data protection requirements. You should also provide your users with clear information about the service you use.
- **Account holder confirmation** - You may be able to rely upon confirmation of user age from an existing account holder who you know to be an adult. For example, if you provide a logged-in or subscription based service, you may allow the main (confirmed adult) account holder to set up child profiles, restrict further access with a password or PIN, or simply confirm the age range of additional account users.
- **Technical measures** – Technical measures which discourage false declarations of age, or identify and close under age accounts, may be useful to support or strengthen self-declaration mechanisms. Examples include neutral presentation of age declaration screens (rather than nudging towards the selection of certain ages), or preventing users from immediately resubmitting a new age if they are denied access to your service when they first self-declare their age.
- **Hard identifiers** – You can confirm age using solutions which link back to formal identity documents or 'hard identifiers' such as a passport. However, we recommend that you avoid giving users no choice but to provide hard identifiers unless the risks inherent in your processing really warrant such an approach. This is because some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults.

We recognise that methods of age assurance will vary depending on whether the service is used by authenticated or non-authenticated users (eg whether users are logged in) and that the risks may also vary

in this context.

What if we need to collect personal data in order to establish age?

You may be able to collect and record personal data which provides an assurance of age yourself. If so, remember that you need to comply with data protection obligations for your collection and retention of that data, including data minimisation, purpose limitation, storage limitation and security obligations.

The key to this is making sure that you only collect the minimum amount of personal data you need to give you an appropriate level of certainty about the age of your individual users, and making sure you don't use personal data collected for the purposes of establishing or estimating age in order to conform to this code for other purposes.

For example, if you use profiling to help you estimate the age of individual users so that you can apply the standards in this code, then you can use that profile information to ensure that you:

- provide age appropriate privacy information and nudges;
- provide high privacy settings for child users by default; and
- don't serve children content deemed detrimental to their health and wellbeing.

You can't however simply re-purpose that information for other purposes, such as targeting children with advertising for products you think they might like, or sending them details of 'birthday offers'. If you want to profile children for this purpose then you need their consent. See the section of this code on [profiling](#) for further detail.

We recognise there is a tension between age assurance and compliance with GDPR, as the implementation of age assurance could increase the risk of intrusive data collection. We do not require organisations to create these counter risks. However, age assurance and GDPR are compatible if privacy by design solutions are used.

Age-assurance tools are still a developing area. The Commissioner will support work to establish clear industry standards and certification schemes to assist children, parents and online services in identifying age-assurance services which comply with data protection standards.


What does applying the standards to all users mean in practice?

If you don't have a level of certainty about the age of your users that is appropriate to the risks to children arising from your data processing, then your alternative is to apply the standards in the code to all users. This should mean that even if you don't really know how old a user is, or if a child has lied about their age, children will still receive some important protections in how their personal data is used.

However, it doesn't mean that you have to ignore any information you do have about the user's age, or that adult users have to be infantilised. It just means that all users will receive some basic protections in how their personal data is used by default.

You should apply the standards in the code in a way that recognises both the information you do have about the users age and the fact that your level of confidence in this information is inadequate to the risks inherent in your processing. For example, providing privacy information that is appropriate to the self-declared age of the user, but giving them the option to access versions written for different age groups as well.

Further reading outside this code

[ICO detailed guidance on DPIAs](#) 

[European guidelines on DPIAs](#) 

[PAS standard 1296 Online Age Checking- code of practice](#) 

4. Transparency

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

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.

What do you mean by 'transparency'?

Transparency is about being clear, open and honest with your users about what they can expect when they access your online service.

Why is it important?

Transparency is key to the requirement under Article 5(1) of the GDPR to process personal data:



"lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"

The GDPR also contains more specific provisions about the information that you must give to data subjects when you process their personal data. These are set out at Article 13 (when you have obtained the personal data directly from the data subject) and Article 14 (when you have not obtained the personal data directly from the data subject).

Article 12 of the GDPR requires you to provide children with this information in a way in which they can access and understand it:



"The controller shall take appropriate measures to provide any information referred to in Article 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject the information may be provided orally, provided that the identity of the data subject is proven by other means."

On a wider level transparency is also intrinsic to the fairness element of Article 5(1). If you aren't clear,

open and honest about the service that you provide and the rules that govern that service, then your original collection and ongoing use of the child's personal data is unlikely to be fair.

How can we make sure that we meet this standard?

Provide clear privacy information

Firstly you need to provide the privacy information set out in Articles 13 and 14 in a clear and prominent place on your online service. You should make this information easy to find and accessible for children and parents who seek out privacy information.

However, it is not sufficient to rely on children or their parents seeking out this privacy information.

Provide 'bite-sized' explanations at the point at which use of personal data is activated

In order to provide children with the specific protection envisaged by Recital 38 you should also provide clear information about what you do with children's personal data in more specific, 'bite-size' explanations, at the point at which the use of the personal data is activated. This is sometimes referred to as a 'just in time notice'. Depending on the age of the child and the risks inherent in the processing, you should also prompt them to speak to an adult before they activate any new use of their data, and not to proceed if they are uncertain.

If you change this setting we will use information about the videos you watch to recommend similar videos to you.

You should talk to a trusted adult before you change this setting, to make sure that you understand and are happy with what this means.

If you don't understand or aren't sure about this then you should leave the setting as it is, and we won't use your information in this way.

More information about what happens to your personal data (information about you) when you use [service name] can be found in our [Privacy Information](#).

I'm not sure about this

I'm OK with this

You should also consider if there are any other points in your user journey when it might be appropriate to provide bite-sized explanations to aid the child's understanding of how their personal data is being used.

Provide clear terms, policies and community standards

All other information you provide for users about your service should also be clear and accessible. This includes terms and conditions, policies and community standards.

In every case you should provide information that is accurate and does not promise protections or standards that are not routinely upheld.

This should help children or their parents make properly informed decisions about whether to provide the information required to access or sign up to your service in the first place, and to continue to use it.

If you believe that you need to draft your terms and conditions in a certain way in order to make them legally robust, then you can provide child-friendly explanations to sit alongside the legal drafting.

Present information in a child friendly way

You should present all this information in a way that is likely to appeal to the age of the child who is accessing your online service.

This may include using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest children, rather than relying solely on written communications.

You may use tools such as privacy dashboards, layered information, icons and symbols to aid children's understanding and to present the information in a child-friendly way. You should consider the modality of your service, and take into account user interaction patterns that do not take place in screen-based environments, as appropriate.

Dashboards should be displayed in a way that clearly identifies and differentiates between processing that is essential to the provision of your service and non-essential or optional processing that the child can choose whether to activate.

Tailor your information to the age of the child

You need to consider how you can tailor the content and presentation of the information you provide depending on the age of the user.

There may be some scenarios in which providing one, simplified, accessible to all, set of information may work. For example, if you are an online retailer which only collects the personal data needed to complete online transactions and deliver goods.

However, in many cases a one-size-fits-all approach does not recognise that children have different needs at different stages of their development. For example, a pre-literate or primary school child might need to be actively deterred from changing privacy settings without parental input, whereas a teenager might be better supported by clear and neutral information which helps them make their own informed decision.


For more information about the developmental needs of children at different ages please see Annex B to this code.

For younger children, with more limited levels of understanding, you may need to provide less detailed information for the child themselves and rely more on parental involvement and understanding. However you should never use simplification with the aim of hiding what you are doing with the child's personal data and you should consider providing detailed information for parents, to sit alongside your child directed


information.

You should make all versions of resources (including versions for parents) easily accessible and incorporate mechanisms to allow children or parents to choose which version they see, or to down-scale or up-scale the information depending on their individual level of understanding.

I don't get this – can you make it a bit easier for me?



This is a bit basic for me – can you give me some more detail?



The following table provides some recommendations. However, they are only a starting point and you are free to develop your own service specific information and user journeys which take account of the risks inherent in your service.

Depending on the size of your organisation, your number of users, and your assessment of risk you may decide to carry out user testing to make sure that the information you provide is sufficiently clear and accessible for the age range in question. You should document the results of any user testing in your DPIA to support your final conclusions and justify the presentation and content of your final resources. If you decide that user testing isn't warranted, then you should document the reasons why in your DPIA.

You should also consider any additional responsibilities you may have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

Age range	Recommendations
0-5 Pre-literate & early literacy	Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents. Provide audio or video prompts telling children to

leave things as they are or get help from a parent or trusted adult if they try and change any high privacy default settings.

6-9
Core primary school years

Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents.

Provide cartoon, video or audio materials to sit alongside parental resources. Explain the basic concepts of online privacy within your service, the privacy settings you offer, who can see what, their information rights, how to be in control of their own information, and respecting other people's privacy. Explain the basics of your service and how it works, what they can expect from you and what you expect from them.

Provide resources for parents to use with their children to explain privacy concepts and risks within your service. Provide resources for parents to use with their children to explain the basics of your service and how it works, what they can expect from you and what you expect from them.

If a child attempts to change a default high privacy setting provide cartoon, video or audio materials to explain what will happen to their information and any associated risks. Tell them to leave things as they are or get help from a parent or trusted adult before they change the setting.

10-12
Transition years

Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents.

Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for children within this age group. Allow children to choose between written and video/audio options. Give children the choice to upscale or downscale the information they see (to materials developed for an older or younger age group) depending on their individual needs.

If a child attempts to change a default high privacy setting provide written, cartoon, video or audio materials to explain what will happen to their information and any associated risks. Tell them to leave things as they are or get help from a parent or trusted adult before they change the setting.

13 -15
Early teens

Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for this age group. Allow them to choose between written and

video/audio options. Give them the choice to upscale or downscale the information they see (to materials developed for an older or younger age group) depending on their individual needs.

If a child attempts to change a default high privacy setting provide written, video or audio materials to explain what will happen to their information and any associated risks. Prompt them to ask for help from a parent or trusted adult and not change the setting if they have any concerns or don't understand what you have told them.

Provide full information in a format suitable for parents to sit alongside the child focused information.

16-17
Approaching adulthood

Provide full information in a format suitable for this age group. Allow them to choose between written and video/audio options. Give them the choice to upscale or downscale the information they see (to materials developed for an older or younger age group) depending on their individual needs.

If a child in this age group attempts to change a default high privacy setting provide written, video or audio materials to explain what will happen to their information and any associated risks. Prompt them to check with an adult or other source of trusted information and not change the setting if they have any concerns or don't understand what you have told them.

Provide full information in a format suitable for parents to sit alongside the child focused information.

Further reading outside this code

[Guide to the GDPR – lawfulness, fairness and transparency](#) 

[Guide to the GDPR – the right to be informed](#) 

5. Detrimental use of data

This code came into force on 2 September 2020, with a 12 month transition period. Organisations should conform by 2 September 2021.

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.

What do you mean by 'the detrimental use of data'?

We mean any use of data that is obviously detrimental to children's physical or mental health and wellbeing or that goes against industry codes of practice, other regulatory provisions or Government advice on the welfare of children.

Why is this important?

Article 5(1)(a) of the GDPR says that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, and Recital 38 that children merit specific protection with regard to the use of their personal data.

Recital 2 to the GDPR states (emphasis added):

“

“The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. **This Regulation is intended to contribute to ... the well-being of natural persons.**”

Recital 75 to the GDPR says that:

“

“The risk to the rights and freedoms of natural persons, or varying likelihood and severity may result from personal data processing which could lead to physical, material or non-material damage, in particular:....where personal data of vulnerable natural persons, in particular children, are processed....”

This means that you should not process children's personal data in ways that are obviously, or have been shown to be, detrimental to their health or wellbeing. To do so would not be fair.

How can we make sure that we meet this standard?

Keep up date with relevant recommendations and advice

As a provider of an online service likely to be accessed by children you should be aware of relevant standards and codes of practice within your industry or sector, and any provisions within them that relate to children. You should also keep up to date with Government advice on the welfare of children in the context of digital or online services. The ICO does not regulate content and is not an expert on matters of children's health and wellbeing. We will however refer to other codes of practice or regulatory advice where relevant to help us assess your conformance to this standard.

Do not process children's personal data in ways that are obviously detrimental or run counter to such advice

You should not process children's personal data in ways that run contrary to those standards, codes or advice and should take account of any age specific advice to tailor your online service to the age of the child. You should take particular care when profiling children, including making inferences based on their personal data, or processing geo-location data.

You should apply a pre-cautionary approach where this has been formally recommended despite evidence being under debate. This means you should not process children's personal data in ways that have been formally identified as requiring further research or evidence to establish whether or not they are detrimental to the health and wellbeing of children.

What codes or advice are likely to be relevant?

Some specific areas where there is relevant guidance, and that are likely to arise in the context of providing your online service are given below.

However, this is not an exhaustive list and you need to identify and consider anything that is relevant to your specific data processing scenario in your DPIA.

Marketing and behavioural advertising

The Committee of Advertising Practice (CAP) publishes guidance about online behavioural advertising which, in addition to providing rules applicable to all advertising, specifically covers advertising to children.

It includes rules which address:

- physical, mental or moral harm to children;
- exploiting children's credulity and applying unfair pressure;
- direct exhortation of children and undermining parental authority; and
- promotions.

It also has rules which govern or prohibit the marketing of certain products, such as high fat, salt and sugar food and drinks and alcohol, to children, and general guidance on transparency of paid-for content and product placement.

Broadcasting

Ofcom has published a code practice for broadcasters which covers the protection of under-18s in the following areas:

- the coverage of sexual and other offences in the UK involving under-18s;
- drugs, smoking, solvents and alcohol;

- violence and dangerous behaviour;
- offensive language;
- sexual material;
- nudity;
- exorcism, the occult and the paranormal; and
- the involvement of people under 18 in programmes.

The press

The Independent Press Standards Organisation (Ipso) has published The Editors' Code of Practice which includes provisions about reporting and children.

Online games

The Office for Fair Trading (OFT) has published principles for online and app-based games which includes provisions about:

- exploiting children's inexperience, vulnerability and credulity, including by aggressive commercial practices; and
- including direct exhortations to children to buy advertised products or persuade their parents or other adults to buy advertised products for them.

Strategies used to extend user engagement

Strategies used to extend user engagement, sometimes referred to as 'sticky' features can include mechanisms such as reward loops, continuous scrolling, notifications and auto-play features which encourage users to continue playing a game, watching video content or otherwise staying online.

Although there is currently no formal Government position on the effect of these mechanisms on the health and wellbeing of children, the UK Chief Medical Officers have issued a 'commentary on screen-based activities on children and young people'. This identifies a need for further research and in the meantime recommends that technology companies 'recognise a precautionary approach in developing structures and remove addictive capabilities.'

Does this mean we can't use features such as rewards, notifications and 'likes' within our service?

No, not all such features rely on the use of personal data and you may have designed your feature taking into account the needs of children and in a way that makes it easy for them to disengage without feeling pressurised or disadvantaged if they do so. However, it does mean that you need to carefully consider the impact on children if you use their personal data to support such features. You should consider both intended and unintended consequences of the data use as part of your DPIA.

Given the precautionary advice from the Chief Medical Officers, designing in data-driven features which make it difficult for children to disengage with your service is likely to breach the Article 5(1)(a) fairness principle of the GDPR. For example, features which use personal data to exploit human susceptibility to reward, anticipatory and pleasure seeking behaviours, or peer pressure.

You should:

- avoid using personal data in a way that incentivises children to stay engaged, such as offering children personalised in-game advantages (based upon your use of the individual user's personal data) in

return for extended play;

- present options to continue playing or otherwise engaging with your service neutrally without suggesting that children will lose out if they don't;
- avoid features which use personal data to automatically extend use instead of requiring children to make an active choice about whether they want to spend their time in this way (data-driven autoplay features); and
- introduce mechanisms such as pause buttons which allow children to take a break at any time without losing their progress in a game, or provide age appropriate content to support conscious choices about taking breaks, such as that provided in the Chief Medical Officers' advice.

Further reading outside the code

[Committee on Advertising Practice guidance](#) 

[The Ofcom Broadcasting Code \(with the Cross-Promotion Code and the On Demand Programme Service Rules\)](#) 

[The Editors' Code of Practice](#)

[OFT principles for online and app-based games](#) 

[UK Chief Medical Officers' commentary on 'screen based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews'](#) 