

Age appropriate design:

a code of practice
for online services

Final version: to be laid in Parliament

Contents

Information Commissioner's foreword	2
Executive summary	3
Code standards	5
About this code	7
Services covered by this code	16
Transitional arrangements	24
Standards of age appropriate design	26
1. Best interests of the child	27
2. Data protection impact assessments	30
3. Age appropriate application	36
4. Transparency	43
5. Detrimental use of data	51
6. Policies and community standards	56
7. Default settings	59
8. Data minimisation	65
9. Data sharing	68
10. Geolocation	71
11. Parental controls	75
12. Profiling	79
13. Nudge techniques	90
14. Connected toys and devices	96
15. Online tools	100
Governance and accountability	105
Enforcement of this code	110
Glossary	114
Annex A: Services covered by the code flowchart	116
Annex B: Age and developmental stages	119
Annex C: Lawful basis for processing	125
Annex D: DPIA template	133

Information Commissioner's foreword

[To be added]

To be laid in Parliament

Executive summary

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

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

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

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

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

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

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

You should follow the standards as part of your approach to complying with data protection law. If you can show us that you conform to these standards then you will conform to the code. The standards are cumulative and interlinked and you must implement them all, to the extent they are relevant to your service, in order to demonstrate your conformity.

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

Code standards

The standards are:

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

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

About this code

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.

In more detail

- [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 [date] and issued on [date 40 days after laid, ignoring parliamentary recess] under section 125 of the DPA 2019. It comes into force on [date 21 days after issue].

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

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?](#)

For more information on the GDPR one-stop-shop principle, see the [EDPB guidelines on the lead supervisory authority](#)

Transitional arrangements

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 [date of end of transition period].

In more detail

[When will the code take effect?](#)

[What should we do about our existing services?](#)

When will the code take effect?

This code was issued on []. It comes into force on []. Providers of relevant ISS likely to be accessed by children will then have 12 months from this date to make sure their services conform to the standards in the code.

From [end of transition period] 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 [end of transition period].

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 [end of transition period]. 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 [end of transition period] 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

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

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

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

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

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?

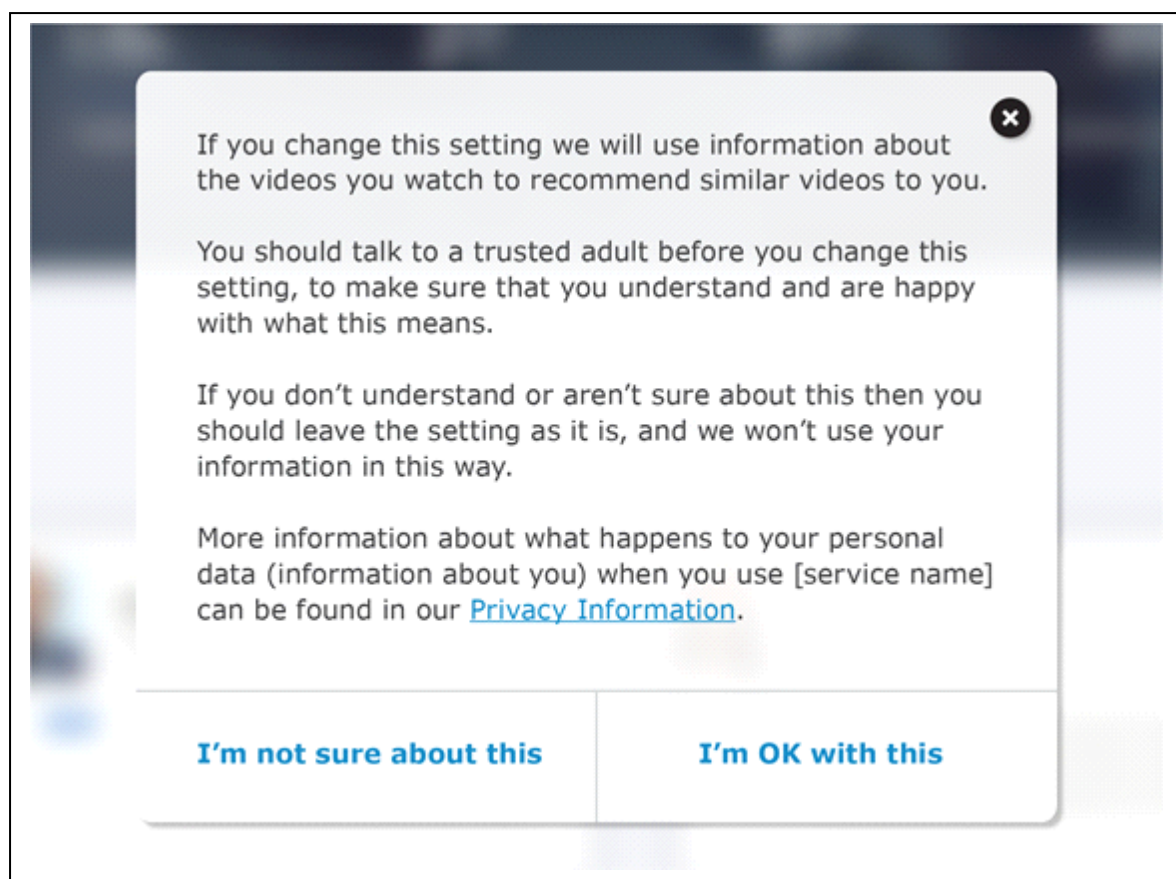
Provide clear privacy information

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.



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.

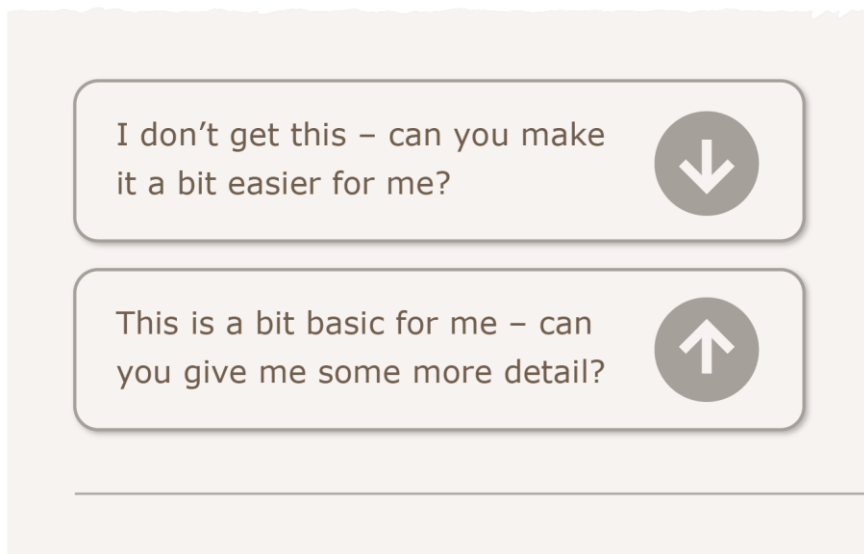
However, in many cases a one-size-fits-all approach does not recognise that children have different needs at different stages of their development. For example, a pre-literate or primary school child might need to be actively deterred from changing privacy settings without parental input, whereas a teenager 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.



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	<p>Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents.</p> <p>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.</p>
6-9 Core primary school years	<p>Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents.</p> <p>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.</p> <p>Provide resources for parents to use with their children to explain privacy concepts and risks within your service.</p> <p>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.</p> <p>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.</p>
10-12 Transition years	<p>Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents.</p> <p>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.</p>

	<p>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.</p>
<p>13 -15 Early teens</p>	<p>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.</p> <p>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.</p> <p>Provide full information in a format suitable for parents to sit alongside the child focused information.</p>
<p>16-17 Approaching adulthood</p>	<p>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.</p> <p>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.</p> <p>Provide full information in a format suitable for parents to sit alongside the child focused information.</p>

--	--

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

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'](#)

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).

What do you mean by ‘upholding your own standards’?

We mean that you need to adhere to your own published terms and conditions and policies.

We also mean that, when you set community rules and conditions of use for users of your service, you need to actively uphold or enforce those rules and conditions.

Why is this important?

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

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

When children provide you with their personal data in order to join or access your service they should be able to expect the service to operate in the way that you say it will, and for you to do what you say you are going to do. If this doesn’t happen then your collection of their personal data may be unfair and in breach of Article 5(1)(a).

Keeping to your own standards should also benefit you by giving children and their parents confidence that they can trust your online service with their personal data.

How can we make sure that we meet this standard?

To some extent this depends on the content of your published terms and conditions, policies and community standards.

However you should follow the overarching principle that you say what you do and do what you say. You should at least ensure that you do the following:

Only use personal data in accordance with your privacy policy

Article 5(1)(b) of the GDPR sets out the 'purpose limitation' principle, that personal data shall be:

"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes..."

Articles 13 and 14 of the GDPR require you to tell data subjects what these purposes are. You do this by providing privacy information, which you may include in a privacy notice, policy or statement.

Article 5(1)(a) of the GDPR requires you to process personal data fairly and transparently.

The combined result of these provisions is that you need to use your privacy information to tell users what you will do with their personal data and why, and then make sure that you follow this through in practice.

Uphold any user behaviour policies

If you have any published rules which govern the behaviour of users of your service then you need to uphold these rules and put in place the systems that you have said you will. So if you say that you actively monitor user behaviour, or offer real time, automated, or human moderation of 'chat' functions, then you need to do so.

If you only rely on 'back end' processes, such as user reporting, to identify behaviour which breaches your policies then you need to have made that very clear in your policies or community standards. This approach also needs to be reasonable given the risks to children of different ages inherent in your service. If the risks are high then 'light touch' or 'back end only' processes to uphold your standards are unlikely to be sufficient.

If you do not have adequate systems to properly uphold your own user behaviour policies then your original collection and continued use of a child's personal data may be unfair and in breach of the GDPR.

Uphold any content or other policies

If you make commitments to users about the content or other aspects of your online service then you need to have systems to ensure that you meet those commitments.

So if you say that the content of your online service is suitable for children within a certain age range then you need to have systems to ensure that it is. If you say that you do not tolerate bullying, then you need to have adequate mechanisms to swiftly and effectively deal with bullying incidents.

Again, if your systems aren't adequate or you don't keep to your promises then your original collection and continued use of the child's personal data may be unfair and in breach of the GDPR.

If you have different policies depending on the age of your users then you need to take account of the age of the child when upholding your 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).

What do you mean by ‘default privacy settings’?

Privacy settings are a practical way for you to offer children a choice over how their personal data is used and protected. You can use them whenever you collect and process children’s personal data in order to ‘improve’ ‘enhance’ or ‘personalise’ their online experience beyond the provision of your core service.

They can cover how children’s personal data is used:

- in an interpersonal sense; the extent to which their personal data is made visible or accessible to other users of your online service;
- by yourself as provider of the online service; for example using personal data to suggest in-app purchases; and
- by third parties; for example to allow third parties to promote or market products.

Default privacy settings govern the use of children’s personal data if the child does not make any changes to the settings when they start using your online service.

Why are they important?

Many children will just accept whatever default settings you provide and never change their privacy settings. This means that it is of the utmost importance that the defaults you set are appropriate for children and provide them with adequate protection in how their personal data is used. For children, it is not enough to allow them to activate high privacy settings, you need to provide them by default (unless you have a compelling reason to do otherwise, taking into account the best interests of the child).

They are also important because of Article 25(2) of the GDPR which provides as follows.

“25(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.”

This means that, by default, you should not:

- collect any more personal data than you need to provide each individual element of your online service; or
- make your users' personal data visible to indefinite numbers of other users of your online service.

You can also use privacy settings to support the exercise of children's data protection rights (such as the rights to object to or restrict processing). And they can give children and parents confidence in their interactions with your online service, and help them explore the implications of allowing you to use their personal data in different ways.

Do we have to provide a privacy setting every time we use a child's personal data?

You should provide privacy settings (set to high privacy by default) to give children control over when and how you use their personal data whenever you can.

It is not necessary however for you to provide a privacy setting for any personal data that you have to process in order to provide your core or most basic service. This is because without this essential processing there is no core service for you to offer. In this circumstance, if the child wishes to access the core service, you cannot offer them a choice over whether their personal data is processed or not.

In order to give children control over when and how their personal data is used, you should provide privacy settings for any processing that is needed to provide additional elements of service that go beyond the core service.

We will look very carefully at any claims that a privacy setting cannot be provided because the personal data is needed to provide the core service. You should follow the spirit not just 'the letter of' the code in this respect and should take care not to abuse the concept of a core service by applying it more widely than is warranted.

See also Annex C to this code 'Lawful basis for processing' which explains the need to differentiate between core and non-core elements of your service in any case, in order to identify an appropriate lawful basis for processing as required by the GDPR.

There may also be some other limited types of processing where it is not appropriate to offer a privacy setting. For example, if you need to process a child's personal data in order to meet a legal obligation (such as a child protection requirement) or to prevent child sexual exploitation and abuse online. It is then not appropriate to offer them a choice over whether their personal data is processed for this purpose or not.

How can we make sure that we meet this standard?

Provide 'high privacy' default settings

If it is appropriate for you to offer a privacy setting, then your default position for each individual privacy setting should be 'high privacy'.

This means that children's personal data is only visible or accessible to other users of the service if the child amends their settings to allow this.

This also means that unless the setting is changed, your own use of the children's personal data is limited to use that is essential to the provision of the service. Any optional uses of personal data, including any uses designed to personalise the service have to be individually selected and activated by the child.

Similarly any settings which allow third parties to use personal data have to be activated by the child.

The exception to this rule is if you can demonstrate that there is a compelling reason for a different default setting taking into account the best interests of the child.

Consider the need for any further intervention at the point at which any setting is changed

Making sure that privacy settings are set to high privacy by default will in itself mitigate the risks to children, as many children will never change their privacy settings from the default position.

Similarly, providing age appropriate explanations and prompts at the point at which a child attempts to change a privacy settings, as required under the transparency standard, will mitigate risk.

However you should also consider whether to put any further measures in place when a child attempts to change a setting. This depends on your assessment of the risks inherent in the processing covered by each setting and could include further age assurance measures. You should use your DPIA to help you assess risks and identify suitable mitigation.

Allow users the option to change settings permanently or just for the current use

If a user does change their settings you should generally give them the option to do so permanently or to return to the high privacy defaults when they end the current session. You should not 'nudge' them towards taking a lower privacy option (for more information on this see the section of this code on Nudge techniques). Slightly different considerations apply for geo-location data which makes the child's location visible to others. This is covered in more detail in the section of this code on [geolocation](#).

Ultimately you need to demonstrate that you have made it easy for a child to maintain or revert to high privacy settings if they wish to do so.

Retain user choices or high privacy defaults when software is updated

If you introduce a software update, (eg to update security measures or introduce new features), then you should retain any privacy settings that the user has applied. If it is not possible to do this (eg if a new aspect or feature to the product or service is introduced, or an existing feature is

significantly changed so the previous privacy settings are no longer relevant) you should set the new setting to high privacy by default.

Allow for different user choices on multi-user devices

If you provide an online service that allows multiple users to access the service from one device, then whenever possible you should allow users to set up their own profiles with their own individual privacy settings. This means that children do not have to share an adult's privacy settings when they share the same device. Profiles could be accessed via screen-based options or using voice recognition technology for voice activated online services.

You should include clear information for the person who sets up or registers the device alerting them to the potential for the personal data of multiple users to be collected.

Are privacy settings a consent mechanism?

For consent to be valid under the GDPR it needs to meet the following definition:

GDPR Article 4(11)

“‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”

If your settings are off by default and the user has to activate the processing by changing the default setting, then you may be able to use privacy settings as part of your mechanism for obtaining consent to your processing under the GDPR. However, you also need to meet the requirements of Article 7 of the GDPR (conditions for consent) and the age verification and parental responsibility verification requirements of Article 8 (these only allow children of 13 or over to provide their own consent), so they won't be enough on their own.

Privacy settings aren't just relevant to consent. You may also use them to give children choice over how their personal data is used if you rely on other lawful bases for processing (such as legitimate interests) which don't have any formal consent requirements.

For more information about lawful bases for processing, including consent, please see the supplementary guidance in Annex C. You may also wish to talk to your DPO if you have one.

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.

What do you mean by 'data minimisation'?

Data minimisation means collecting the minimum amount of personal data that you need to deliver an individual element of your service. It means you cannot collect more data than you need to provide the elements of a service the child actually wants to use.

Why is it important?

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

"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"

Article 25 of the GDPR provides that this approach shall be applied by default to 'each specific purpose of the processing'.

It sits alongside the 'purpose limitation' principle set out at Article 5(1)(b) of the GDPR which states that the purpose for which you collect personal data must be 'specified, explicit and legitimate' and the storage limitation principle set out in Article 5(1)(e) which states that personal data should be kept 'no longer than is necessary' for the purposes for which it is processed.

How can we make sure that we meet this standard?

Identify what personal data you need to provide each individual element of your service

The GDPR requires you to be clear about the purposes for which you collect personal data, to only collect the minimum amount of personal data you need for those purposes and to only store that data for the minimum amount of time you need it for. This means that you need to differentiate between each individual element of your service and consider what personal data you need, and for how long, to deliver each one.

Example

You offer a music download service.

One element of your service is to allow users to search for tracks they might want to download.

Another element of your service is to provide recommendations to users based on previous searches, listens and downloads.

A further element of your service is to share what individual users are listening to with other groups of users

These are all separate elements of your overall service. The personal data that you need to provide each element will vary.

Give children choice over which elements of your service they wish to use

You should give children as much choice as possible over which elements of your service they wish to use and therefore how much personal data they need to provide.

This is particularly important for your collection of personal data in order to 'improve' 'enhance' or 'personalise' your users' online experience beyond the provision of your core service.

You should not 'bundle in' your collection of children's personal data in order to provide such enhancements with the collection of personal data you need to provide the core service, as you are effectively collecting personal data for different purposes. Neither should you bundle together several additional elements or enhancements of the service. You should give children a choice

as to whether they wish their personal data to be used for each additional purpose or service enhancement. You can do this via your default privacy settings, as covered in the earlier section of this code.

Only collect personal data when the child is actively and knowingly using that element of your service

You should only collect the personal data needed to provide each element of your service when the child is actively and knowingly engaged with that element of the service.

Example:

It is acceptable to collect a child's location when they are using a maps based element of your service to help them find their way to a specified destination, and if you provide an obvious sign so that they know their location is being tracked.

It is not acceptable to continue to track their location after they have closed the map or reached their destination.

Further reading outside the code:

[Guide to GDPR – data minimisation](#)

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.

What do you mean by 'data sharing'?

Data sharing usually means disclosing personal data to third parties outside your organisation. It can also cover the sharing of personal data between different parts of your own organisation, or other organisations within the same group or under the same parent company.

Data sharing can be done routinely (for example the provider of an educational app routinely sharing data with the child's school) or in response to a one-off or emergency situation (for example sharing a child's personal data with the police for safeguarding reasons).

Data sharing includes making a child's personal data visible to a third party.

Why is it important?

It is important because if you share children's personal data with third parties or with other parts of your own organisation it needs to be fair to the child to do so. Sharing children's personal data with third parties, including sharing data inferred or derived from their personal data, can expose children to risks arising from their processing of personal data, which go beyond those inherent in your own processing.

The GDPR provides that:

"5(1) Personal data shall be:

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

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”.

Articles 13 and 14 of the GDPR require you to tell data subjects who you share the personal data with (the recipients or categories of recipients of the personal data).

How can we make sure that we meet this standard?

Consider the best interests of the child

The best interests of the child should be a primary consideration for you whenever you contemplate sharing children’s personal data.

If you have already made sure that your privacy settings are set to ‘high privacy’ by default, then the amount of data sharing that takes place should already be limited; with children having to actively change the default settings to allow you to share their personal data in many circumstances.

You should not share personal data if you can reasonably foresee that doing so will result in third parties using children’s personal data in ways that have been shown to be detrimental to their wellbeing. You should obtain assurances from whoever you share the personal data with about this, and undertake due diligence checks as to the adequacy of their data protection practices and any further distribution of the data.

Any default settings related to data sharing should specify the purpose of the sharing and who the data will be shared with. Settings which allow general or unlimited sharing will not be compliant.

Ultimately, it is up to the person you have shared the data with to ensure they comply with the requirements of the GDPR (in their role as a data controller for the personal data they receive). However, you are responsible for ensuring that it is fair to share the personal data in the first place. You should not share personal data unless you have a compelling reason to do so, taking account of the best interests of the child.

One clear example of a compelling reason is data sharing for safeguarding purposes, preventing child sexual exploitation and abuse online, or for the purposes of preventing or detecting crimes against children such as online grooming.

An example that is unlikely to amount to a compelling reason for data sharing is selling on children's personal data for commercial re-use.

Consider the specific issues and risks raised at each stage of your DPIA

You should assess the issues and risks raised at each individual step of your DPIA process. These steps are set out and explained in the section of this code on DPIAs.

Further reading outside the code

For further reading on data sharing see our Data Sharing Code of Practice

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), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others should default back to 'off' at the end of each session.

What do you mean by 'geolocation data'?

Geolocation data means data taken from a user's device which indicates the geographical location of that device, including GPS data or data about connection with local wifi equipment.

Why is it important?

Recital 38 to the GDPR states that:

"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"

The use of geolocation data in relation to children is of particular concern. This is because the ability to ascertain or track the physical location of a child carries with it the risk that the data could be misused to compromise the physical safety of that child. In short it can make children vulnerable to risks such as abduction, physical and mental abuse, sexual abuse and trafficking.

Persistent sharing of location may also mean that children have a diminished sense of their own private space which may affect the development of their sense of their own identity. It may potentially fail to respect the child's rights under the UNCRC to privacy, freedom of association, and freedom from economic exploitation, irrespective of threats to their physical safety.

Should all geolocation services be controlled by a privacy setting?

For any geolocation data you need to process in order to provide your core service, it is not appropriate to have a privacy setting (as without the processing there is no core service to provide). For example, map services may need to know the user location in order to properly display the required map or direct the user to their chosen destination.

However, you should offer children control over whether and how their personal data is used whenever you can. So any geolocation services that go over and above your core service should be subject to a privacy setting. For example, enhanced mapping services that make recommendations for places to visit based on location.

How can we make sure that we meet this standard?

Ensure geolocation options are off by default

Any geolocation privacy setting you do provide should be switched off by default; with children having to actively change the default setting to allow their geolocation data to be used. The exception to this is if you can demonstrate a compelling reason for a geolocation option to be switched on by default, taking into account the best interests of the child. For example you may be able to argue that metrics needed to measure demand for regional services may be sufficiently un-intrusive to be warranted (taking into account the best interests of the child).

You should also consider at what level of granularity the location needs to be tracked to provide each element of your service. Do not collect more granular detail than you actually need, and offer different settings for different levels of service if appropriate.

Make it obvious to the child that their location is being tracked

You should provide information at the point of sign-up, and each time the service is accessed that alerts the child to the use of geolocation data and prompts them to discuss this with a trusted adult if they don't understand what it means.

You should also provide a clear indication of when the child's location is and isn't being tracked (eg by use of a clear symbol visible to the user), and ensure that location tracking can't be left on inadvertently or by mistake.

Revert settings which make the child's location visible to others to 'off' after each use

You should make sure that any option which makes the child's location visible to others is subject to a privacy setting which reverts to 'off' after each session. The exception to this is if you can demonstrate that you have a compelling reason to do otherwise taking into account the best interests of the child.

What about PECR?

If the geolocation data that you are processing also meets the definition of 'location data' in PECR then you should refer to our Guide to PECR for further guidance, as there are PECR specific requirements you have to meet.

Location data is defined as:

"any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—

- (f) the latitude, longitude or altitude of the terminal equipment;
- (g) the direction of travel of the user; or
- (h) the time the location information was recorded".

In other words, it is information collected by a network or service about where the user's phone or other device is or was located. For example, tracing the location of a mobile phone from data collected by base stations on a mobile phone network.

The PECR rules do not generally include GPS-based location information from smartphones, tablets, sat-navs or other devices, as this data is created and collected independently of the network or service provider. Neither does it include location information collected at a purely local level (eg by wifi equipment installed by businesses offering wifi on their premises).

Further reading outside this code

[Guide to PECR – location data](#)

To be laid in Parliament

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.

What do you mean by 'parental controls'?

Parental controls are tools which allow parents or guardians to place limits on a child's online activity and thereby mitigate the risks that the child might be exposed to. They include things such as setting time limits or bedtimes, restricting internet access to pre-approved sites only, and restricting in-app purchases. They can also be used to monitor a child's online activity or to track their physical location.

Why are they important?

They are important because they can be used to support parents in protecting and promoting the best interests of their child, a role recognised by the UNCRC and discussed in the section of this code on the best interests of the child.

However they also impact on the child's right to privacy as recognised by Article 16 of the same convention and on their rights to association, play, access to information and freedom of expression. Children who are subject to persistent parental monitoring may have a diminished sense of their own private space which may affect the development of their sense of their own identity. This is particularly the case as the child matures and their expectation of privacy increases.

Article 5(1)(a) of the GDPR requires any processing of personal data related to their use to be lawful, fair and transparent.

"5(1) Personal data shall be:

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

How can we make sure that we meet this standard?

Make it clear to the child if parental controls are in place and if they are being tracked or monitored

If you provide parental controls then you should provide age appropriate information so that the child knows that parental controls are in place.

If your online service allows parental monitoring or tracking of a child, you should provide age appropriate resources to explain the service to the child so that they are aware that their activity is being monitored by their parents or their location tracked. You should provide a clear and obvious sign for the child (such as a lit up icon) which lets them know when monitoring or tracking is active.

You should also provide parents with information about the child's right to privacy under the UNCRC and resources to support age appropriate discussion between parent and child.

The following table provides some guidelines on the type of information you might wish provide and how you might provide it. They are only a starting point and you are free to develop your own, service specific, user journeys that follow the principle in the headline standard.

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 audio or video materials for the child to explain that their parent is being told what they do online to help keep them safe.

	<p>Provide materials for parents explaining the child's right to privacy under the UNCRC and how their expectations about this are likely to increase as they get older.</p> <p>Provide a clear and obvious sign that indicates when monitoring or tracking is active.</p>
6-9 Core primary school years	<p>Provide audio or video materials for the child to explain that their parent is being told where they are and/or what they do online to help keep them safe.</p> <p>Provide materials for parents explaining the child's right to privacy under the UNCRC and how their expectations about this are likely to increase as they get older.</p> <p>Provide resources to help parents explain the service to their child and discuss privacy with them.</p> <p>Provide a clear and obvious sign that indicates when monitoring or tracking is active.</p>
10-12 Transition years	<p>Provide audio or video materials for the child to explain that their parent is being told where they are and/or what they do online to help keep them safe.</p> <p>Provide materials for parents explaining the child's right to privacy under the UNCRC and how their expectations about this are likely to be increasing now they are getting older.</p> <p>Provide resources to help parents explain the service to their child and discuss privacy with them.</p> <p>Provide resources suitable for the child to use independently which explain the service and discusses privacy rights.</p> <p>Provide a clear and obvious sign that indicates when monitoring or tracking is active.</p>

<p>13 -15 Early teens</p>	<p>Provide audio, video or written materials for the child to explain how your service works and the balance between parental and child privacy rights.</p> <p>Provide materials for parents explaining the child's right to privacy under the UNCRC.</p> <p>Provide a clear and obvious sign that indicates when monitoring or tracking is active.</p>
<p>16-17 Approaching adulthood</p>	<p>Provide audio, video or written materials for the child to explain how your service works and the balance between parental and child privacy rights.</p> <p>Provide materials for parents explaining the child's right to privacy under the UNCRC.</p> <p>Provide a clear and obvious sign that indicates when monitoring or tracking is active.</p>

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).

What do you mean by ‘profiling’?

Profiling is defined in the GDPR:

“ any form of automated processing of personal data consisting of the use of person data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements”

Profiling can be used for a wide range of purposes. It can be used extensively in an online context to suggest or serve content to users, to determine where, when and how frequently that content should be served, to encourage users towards particular behaviours, or to identify users as belonging to particular groups. It can also be used to help establish or estimate the age of a user (as detailed in the standard on age appropriate application), or for child protection, countering terrorism, or the prevention of crime.

Profiles are usually based on a user’s past online activity or browsing history. They can be created using directly collected personal data or by drawing inferences (eg preferences or characteristics inferred from associations with other users or past online choices).

Content feeds based on profiling can include advertising content, content provided by other websites, downloads, content generated by other internet

users, written, audio or visual content. Profiling may also be used to suggest other users to 'connect with' or 'follow'.

Why is it important?

Profiling is mentioned in Recital 38 to the GDPR as an area in which children merit specific protection with regard to the use of their personal data.

There are also specific rules at Article 22 of the GDPR about decisions (including profiling) which are based solely on the automated processing of personal data, and which have a legal or similarly significant effect on the data subject.

"22(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her"

Recital 71 to the GDPR states that such decisions 'should not concern a child'.

The lawfulness, fairness and transparency principle at Article 5(1) is also relevant because this is an area of largely 'invisible processing' in which it is difficult for children to understand how their personal data is being used, and what the consequences of that use might be.

"5(1) Personal data shall be
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"

Some profiling may be relatively benign, for example personalisation of a 'walled garden' online environment to incorporate an animal theme in the displayed content. Other profiling, such as content feeds which gradually take the child away from their original area of interest into other less suitable content, raise much more significant concerns.

Should all profiling be controlled by a privacy setting?

It is important to remember that 'off by default' does not mean that profiling is not possible or banned. Following the safeguards and steps set

out in this section, which could include effective consent, can enable profiling using children's data to take place, safely and fairly.

There is no point in offering a privacy setting if the profiling is essential to the provision of the core service that the child has requested. This is because if the profiling were turned off there would be no residual service left for the child to use. This concept should be interpreted narrowly, eg that it is completely intrinsic to the service.

However, whenever you can, you should offer children control over whether and how their personal data is used. So most profiling should be subject to a privacy setting. If you can provide a core or residual service without profiling, then you should provide a privacy setting for any additional aspects of your service which rely on profiling.

You should always provide a privacy setting for behavioural advertising which is used to fund a service, but is not part of the core service that the child wishes to access. Although there may be some limited examples of services where behavioural advertising is part of the core service (eg a voucher or 'money off' service), we think these will be exceptional. In most cases the funding model will be distinct from the core service and so should be subject to a privacy setting that is 'off' by default.

There may also be some other limited circumstances in which it won't be appropriate for you to offer a privacy setting over profiling. For example, if you are profiling in order to meet a legal or regulatory requirement (such as a safeguarding or child protection requirement), to prevent child sexual exploitation or abuse online or to age assure so you can properly apply the provisions of this code to child users.

How does this fit with PECR requirements?

Profiling may rely on the use of cookies and similar technologies in order to store or 'remember' the information about a user's past online activity.

A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

PECR requires that you provide users with clear and comprehensive information about your use of cookies and obtain prior consent for any that are 'non-essential'.

So if you use cookies for the purposes of profiling you need to consider PECR rules for the setting of the cookie, and the GDPR and this code for the underlying processing of personal data (profiling) that the cookie supports or enables.

Profiling and non-essential cookies

If the cookie isn't essential to provide the service that the child wants to access, then the underlying profiling it facilitates normally needs to be subject to a privacy setting. This gives the child control over whether their personal data is used for this purpose.

You need consent for the cookie as well as a GDPR lawful basis for processing for the underlying processing (in practice this may also be consent).

Cookies, profiling, and your core services

If the cookie is essential to the provision of your core service then it is likely that the underlying profiling that the cookie enables is too. In this circumstance providing a privacy setting which allows the child to control whether their personal data is used for this purpose won't be appropriate. You need a lawful basis (other than consent) for the underlying processing (profiling) and won't need consent for the cookie.

Cookies, profiling and your non-core services

Cookies may also be essential for providing your non-core services. However, as these are optional elements of your service you firstly need to provide a privacy setting which gives the child control over whether they wish their personal data to be processed in order to access them.

If the child decides to do so, then you do not need consent for the use of the cookie – as the child is specifically requesting to access part of your service and the cookie is strictly necessary for this purpose.

You do however need a lawful basis for the underlying processing.

Cookies, profiling, and age estimation or age assurance

You may also use cookies for profiling that intends to meet the implied age verification requirements of Article 8 of the GDPR, or to age assure in order to properly apply the standards of this code. For more detail about the Article 8 requirements see [Annex C Lawful bases for processing](#).

In this circumstance, the purpose you use the cookies for is regarded as essential for the service, as you need to do so to provide an age appropriate service and comply with the GDPR. Provided that the cookie in question is solely used for this purpose, and not for any other purpose, then the child does not need to consent to the cookie.

For more information about cookies, and when a cookie is essential and non-essential, see our guidance on [Cookies and similar technologies](#).

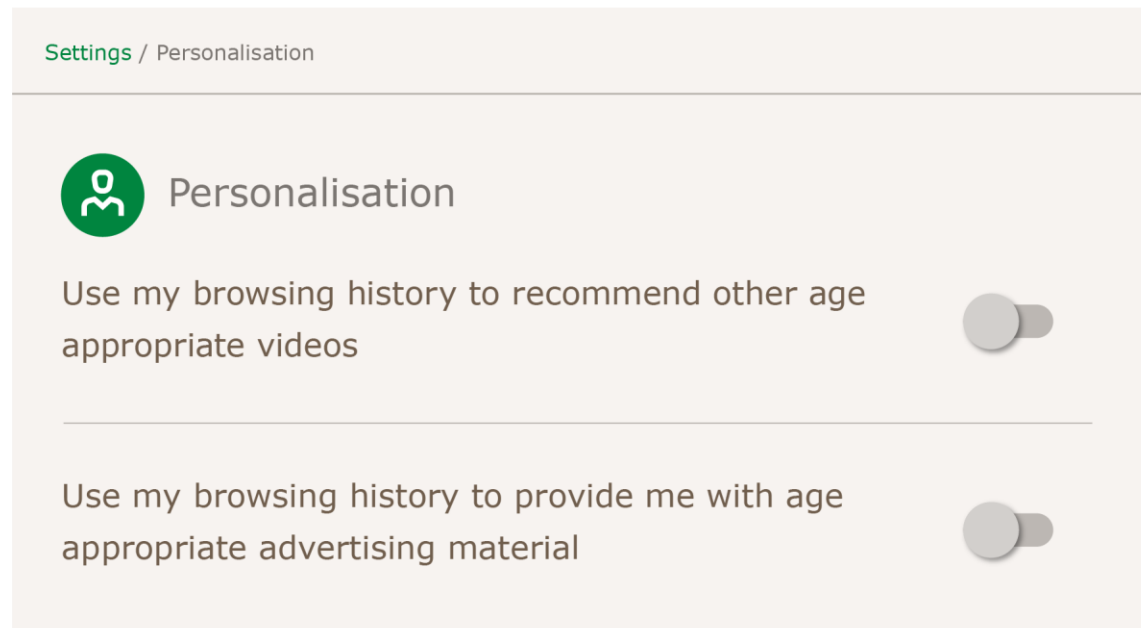
How can we make sure that we meet this standard?

Differentiate between different types of profiling for different purposes

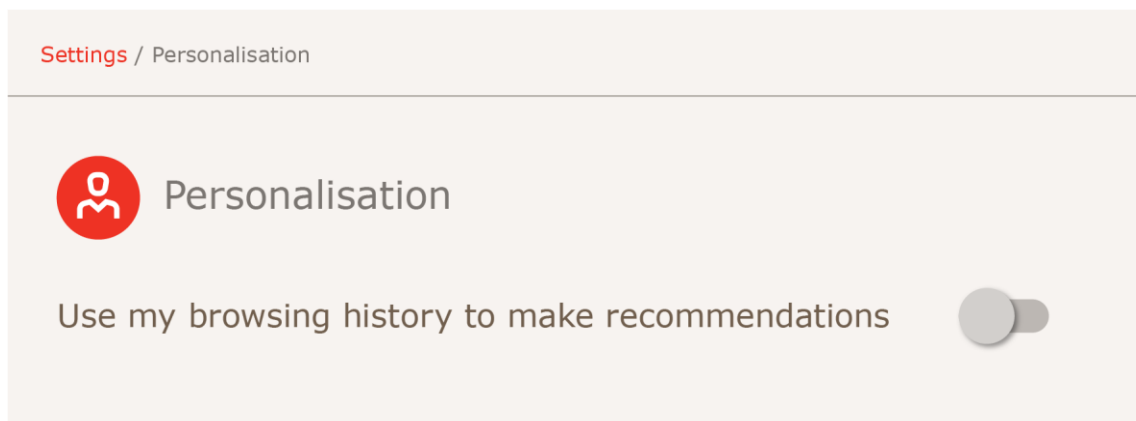
Because profiling can be used to serve a wide range of purposes it is particularly important to be clear about the purposes for which your service uses personal data to profile its users, and to differentiate between them. Catch-all purposes, such as 'providing a personalised service' are not specific enough.

Where it is appropriate to offer privacy settings then you should offer separate settings for each different type of profiling. It is not acceptable to bundle different types of profiling together under one privacy setting, or to bundle in profiling with processing for other purposes.

Acceptable practice:



Unacceptable practice:



Ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise)

You need to switch any options within your service which rely on profiling off by default, unless you can demonstrate a compelling reason why this should not be the case, taking account of the best interests of the child. You need to assess this in the specific circumstances of your processing.

In practice it is likely to mean that any non-essential features that rely on profiling and that you provide for commercial purposes are subject to a privacy setting which is switched off by default.

In the case of any profiling you do for the purposes of behavioural advertising, which is facilitated by cookies, this approach is supported by the comments of the EDPB. EDPB have indicated that 'legitimate interests' is unlikely to provide a valid lawful basis for processing for this purpose which means that consent is your only viable basis for processing. As valid consent has to be 'opt in', allowing such profiling 'by default' is not an option. You also need to comply with the Article 8 GDPR requirements for parental consent if the child is under the age of 13. For more information about lawful bases for processing and Article 8 requirements see Annex C.

However, you may have a compelling argument that you need to switch profiling options for other purposes on by default.

For example, it may be appropriate for profiling for the purposes of ensuring that a service is accessible to a disabled child (eg identifying that a child has an ongoing need for a subtitled, signed or other supported service) to be switched on by default.

You may be able to demonstrate that profiling for the purposes of informing news content feeds should be allowed by default, in order to recognise the rights of children to access information. Although you still need consent to set the cookies that support the profiling in accordance with PECR requirements. This is more likely to be the case if you can demonstrate that you conform with existing regulatory codes of practice which govern media content and practices (such as The Editors' Code of Practice) and have editorial control over the content that children will be shown as a result of the profiling. It is unlikely to apply if you do not have such editorial control or adhere to other regulatory controls. See also our FAQs for the news media.

Provide appropriate interventions at the point at which any profiling is activated

At the point any profiling options are turned on, you need to provide age appropriate information about what will happen to the child's personal data and any risks inherent in that processing.

You should also provide age appropriate prompts to seek assistance from an adult and not to activate the profiling if they are uncertain or don't understand.

Depending on your assessment of risk and the age of the child you may wish to make further interventions, which might include further age assurance measures.

If profiling is on ensure that you put appropriate measures in place to safeguard the child (in particular from inappropriate content)

If your online service uses any profiling then you need to take appropriate steps to make sure that this does not result in harm to the child.

In practice this means that if you profile children (using their personal data) in order to suggest content to them, then you need suitable measures in place to make sure that children aren't served content which is detrimental to their physical or mental health or wellbeing, taking into account their age. As covered in the section of this code on DPIAs, testing your algorithms should assist you in assessing the effectiveness of your measures.

Such measures could include contextual tagging, robust reporting procedures, and elements of human moderation. It could also include your own editorial controls over the content you display, including adherence to codes of conduct or other regulatory provisions (such as compliance with The Editors' Code of Practice, or the Ofcom Broadcasting Code). We recognise the importance of the rights of children to access information from the media, and the societal and developmental benefits of children being able to engage in current affairs and the world around them. We would therefore accept that adherence to editorial or broadcasting codes of conduct negate the need for providers of online news to take any additional steps in relation to news content for children. See also our FAQs for the news media.

If you are using children's personal data to automatically recommend content to them based on their past usage/browsing history then you have a responsibility for the recommendations you make. This applies even if the content itself is user generated. In data protection terms, you have a greater responsibility in this situation than if the child were to pro-actively search out such content themselves. This is because it is your processing of the personal data that serves the content to the child. Data protection law doesn't make you responsible for third party content but it does make you responsible for the content you serve to children who use your service, based on your use of their personal data.

Your general approach should be that if the content you promote or the behaviours your features encourage are obviously detrimental, or are recognised as harmful to the child, in one context (eg marketing rules, film classification, advice from official Government sources such as Chief Medical Officers' advice, PEGI ratings) then you should assume that the same type of content or behaviour is harmful in other contexts as well. Where evidence is inconclusive you should apply the same precautionary principle.

Content or behaviours that may be detrimental to children's health and wellbeing (taking into account their age) include:

- advertising or marketing content that is contrary to CAP guidelines on marketing to children;
- film or on-demand television content that is classified as unsuitable for the age group concerned;
- music content that is labelled as parental advisory or explicit;

- pornography or other adult or violent content;
- user generated content (content that is posted by other internet users) that is obviously detrimental to children's wellbeing or is formally recognised as such (eg pro-suicide, pro-self harm, pro-anorexia content. Content depicting or advocating risky or dangerous behaviour by children); and
- strategies used to extend user engagement, such as timed notifications that respond to inactivity.

Ultimately, if you believe that it is not feasible for you to put suitable measures in place, then you are not be able to profile children for the purposes of recommending online content. In this circumstance you need to make sure that children cannot change any privacy settings which allow this type of profiling.

Similarly, if you cannot put suitable measures in place to safeguard children from harms arising from profiling for other purposes (such as profiling to promote certain behaviours), you should not profile children for these purposes either.

How does this fit with other rules on restricting access to content for children?

You may need to take account of other rules on restricting access to content in order to ensure that you don't use children's personal data in ways that have been shown to be detrimental to their wellbeing (for more detail see the standard on [detrimental use of data](#)).

The CAP code requires that when advertising is targeted through the use of personal data, advertisers must show that they have taken reasonable steps to reduce the likelihood of those who are, or are likely to be, in a protected age category being exposed to age-restricted marketing content.

The Ofcom On Demand Programme Service Rules require providers of 'on demand' content to only make certain content ('specially restricted material') available, if it can do so in a way that ensures that those under the age of 18 will not normally be able to see or hear it.

The Audiovisual Media Services Directive 2018 (AVMSD) (if implemented in the UK) will require 'video sharing platform services' to use proportionate measures in relation to how they organise the content they share, to protect minors from content which might impair their physical, mental or moral development.

We consider that it is consistent with these provisions to only allow children's personal data to be used to determine content feeds if you can put suitable measures in place to guard against them being served content that is detrimental to their health and wellbeing

The AVMSD also requires that you should not use personal data collected or generated for the purposes of protecting minors from content which might impair their physical, mental or moral development for commercial purposes such as direct marketing, profiling and behaviourally targeted advertising.

We consider that this requirement is consistent with the purpose limitation principle of the GDPR and with our guidance in the sections of this code on age appropriate application - What if we need to collect personal data in order to establish age? It doesn't mean that services within the scope of the AVMSD can't ever process personal data for commercial purposes. It just means that you can't use personal data collected for one purpose for another. If such services wish to profile children for the purpose of behavioural advertising you will need the child's (or parent's) consent. For more information on consent see [Annex C Lawful bases for processing](#).

We will work with other regulators as necessary where issues of regulatory consistency arise.

Further reading outside this code

[The Editors' Code of Practice](#)

The Ofcom Broadcasting Code (with the Cross-promotion Code and the on Demand Programme Service Rules)

Directive (EU) 2018/1808 amending Directive 2010/13/EU (Audiovisual Media Services Directive) and the [UK government's Audiovisual Media Services Consultation Document](#)

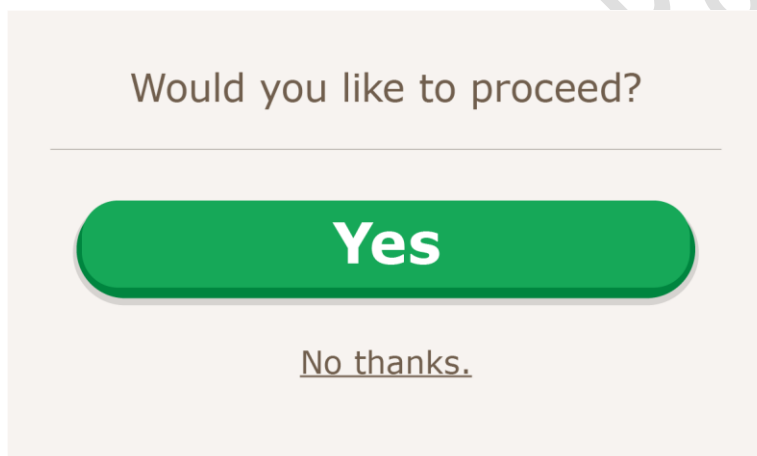
Age Appropriate Design Code FAQs for the news media

13. Nudge techniques

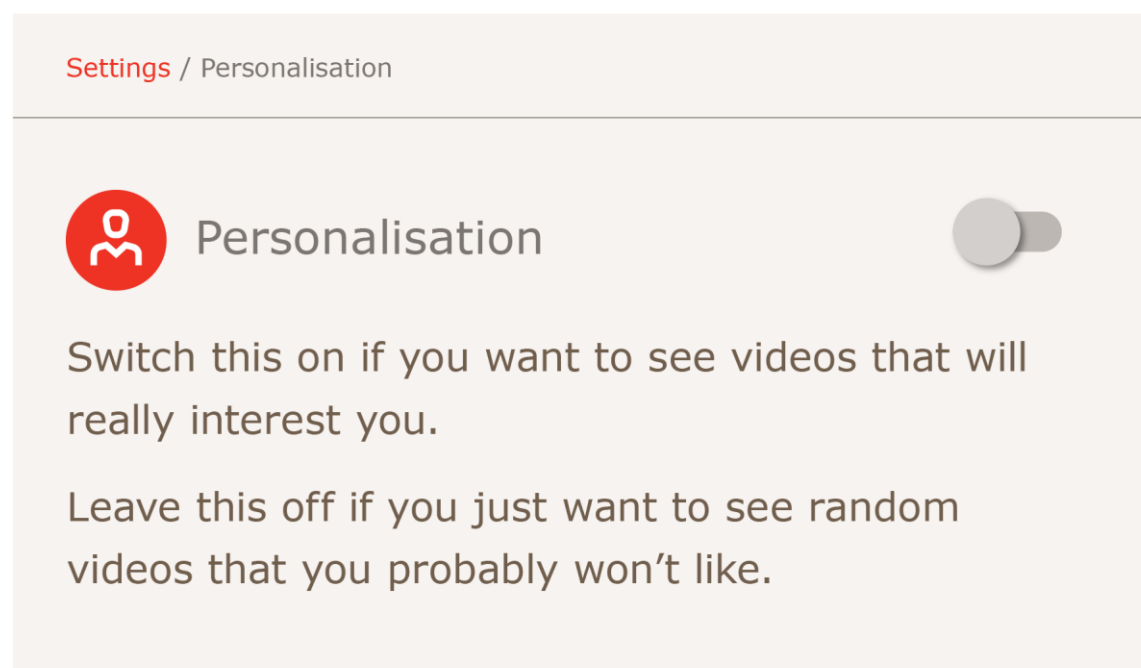
Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.

What do you mean by ‘nudge techniques’?

Nudge techniques are design features which lead or encourage users to follow the designer’s preferred paths in the user’s decision making. For example, in the graphic below the large green ‘yes’ button is presented far more prominently than the small print ‘no’ option, with the result that the user is ‘nudged’ towards answering ‘yes’ rather than ‘no’ to whatever option is being presented.



In the next example the language used to explain the outcomes of two alternatives is framed more positively for one alternative than for the other, again ‘nudging’ the user towards the service provider’s preferred option.



A further nudge technique involves making one option much less cumbersome or time consuming than the alternative, therefore encouraging many users to just take the easy option. For example providing a low privacy option instantly with just one 'click', and the high privacy alternative via a six click mechanism, or with a delay to accessing the service.

Why is this important?

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

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

Recital 38 to the GDPR states that:

"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..."

The employment of nudge techniques in the design of online services can be used to encourage users, including children, to provide an online service with more personal data than they would otherwise volunteer. Similarly it can be used to lead users, particularly children, to select less privacy-enhancing choices when personalising their privacy settings.

Using techniques based on the exploitation of human psychological bias in this way goes against the 'fairness' and 'transparency' provisions of the GDPR as well as the child specific considerations set out in Recital 38.

How can we make sure that we meet this standard?

Do not use nudge techniques to lead children to make poor privacy decisions

You should not use nudge techniques to lead or encourage children to activate options that mean they give you more of their personal data, or turn off privacy protections.

You should not exploit unconscious psychological processes to this end (such as associations between certain colours or imagery and positive outcomes, or human affirmation needs).

You should not use nudge techniques that might lead children to lie about their age. For example pre-selecting an older age range for them, or not allowing them the option of selecting their true age range.

Use pro-privacy nudges where appropriate

Taking into account the best interests of the child as a primary consideration, your design should support the developmental needs of the age of your child users.

Younger children, with limited levels understanding and decision making skills need more instruction based interventions, less explanation, unambiguous rules to follow and a greater level of parental support. Nudges towards high privacy options, wellbeing enhancing behaviours and parental controls and involvement should support these needs.

As children get older your focus should gradually move to supporting them in developing conscious decision making skills, providing clear explanations of functionality, risks and consequences. They will benefit from more neutral interventions that require them to think things through. Parental support may still be required but you should present this as an option alongside signposting to other resources.

Consider nudging to promote health and wellbeing

You may also wish to consider nudging children in ways that support their health and wellbeing. For example, nudging them towards supportive resources or providing tools such as pause and save buttons.

If you use personal data to support these features then you still need to make sure your processing is compliant (including having a lawful basis for processing and have providing clear privacy information), but subject to this it is likely that such processing will be fair.

The table below gives some recommendations that you might wish to apply to children of different ages. Although again you are free to develop your own, service specific, user journeys that follow the principle in the headline standard.

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	<p>Provide design architecture which is high-privacy by default. If change of default attempted nudge towards maintaining high privacy or towards parental or trusted adult involvement.</p> <p>Avoid explanations – present as rules to protect and help. Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing.</p> <p>Nudge towards wellbeing enhancing behaviours (such as taking breaks).</p> <p>Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).</p>
6-9 Core primary school years	<p>Provide design architecture which is high-privacy by default. If change of default attempted nudge towards maintaining high privacy or parental or trusted adult involvement.</p>

	<p>Provide simple explanations of functionality and inherent risk, but continue to present as rules to protect and help.</p> <p>Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing.</p> <p>Nudge towards wellbeing enhancing behaviours (such as taking breaks).</p> <p>Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).</p>
10-12 Transition years	<p>Provide design architecture which is high-privacy by default. If change of default attempted provide explanations of functionality and inherent risk and suggest parental or trusted adult involvement.</p> <p>Present option in ways that encourage conscious decision making.</p> <p>Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks.</p> <p>Nudge towards wellbeing enhancing behaviours (such as taking breaks).</p> <p>Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).</p>
13 -15 Early teens	<p>Provide design architecture which is high-privacy by default.</p> <p>Provide explanations of functionality and inherent risk.</p> <p>Present options in ways that encourage conscious decision making.</p> <p>Signpost towards sources of support including parents.</p> <p>Consider further interventions depending on the risks.</p>

	<p>Suggest wellbeing enhancing behaviours (such as taking breaks).</p> <p>Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).</p>
16-17 Approaching adulthood	<p>Provide design architecture which is high-privacy by default.</p> <p>Provide explanations of functionality and inherent risk.</p> <p>Present options in ways that encourage conscious decision making.</p> <p>Signpost towards sources of support including parents.</p> <p>Suggest wellbeing enhancing behaviours (such as taking breaks).</p> <p>Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).</p>

14. Connected toys and devices

If you provide a connected toy or device, ensure you include effective tools to enable conformance to this code.

What do you mean by ‘connected toys and devices’?

These are children’s toys and other devices which are connected to the internet. They are physical products which are supported by functionality provided through an internet connection. For example:

- a talking teddy bear with a microphone that records what the child is saying and then sends this data back to your servers so that you can use it to personalise the teddy bear’s responses;
- a fitness band that records the child’s level of physical activity and then transmits this back to your servers so the child can then access activity reports via a fitness app; or
- a ‘home hub’ interactive speaker device that provides internet based services via a voice recognition service.

You need to conform to the standards in this code if you provide a toy or device which collects and personal data and transmits it via a network connection in this way. If you provide electronic toys or devices that do not connect to the internet, and only store personal data within the device itself, this code does not apply to you as you do not have access to any personal data.

Why is this important?

Connected toys and devices raise particular issues because their scope for collecting and processing personal data, via functions such as cameras and microphones, is considerable. They are often used by multiple people of different ages, and by very young children without adult supervision. Delivering transparency via a physical rather than a screen-based product can also be a particular challenge.

Nevertheless you still have a responsibility to meet GDPR requirements and to ensure your processing is lawful, fair and transparent as required by Article 5(1); so you need to make sure you have tools to enable you to conform with this code.

How can we make sure that we meet this standard?

Be clear about who is processing the personal data and what their responsibilities are

If you provide a connected toy or device then you need to be clear about who will process the personal data that it transmits via the network connection and what their data protection responsibilities are.

If you provide both the physical product and the online functionality that supports it, then you are solely responsible for ensuring compliant processing. If you outsource or 'buy in' the online functionality or 'connected' element of the device then whoever provides this aspect of the overall product will also have responsibilities. The extent of these will vary depending on whether they are a 'processor' acting only on your behalf, or a 'controller' in their own right.

However, you cannot absolve yourself of your data protection obligations by outsourcing the 'connected' element of your toy or device to someone else. If you provide a connected toy or device then you need to comply with the GDPR and follow this code, and make sure that any third parties you use to deliver your overall product do so too.

This is particularly important when you are making sure that the product incorporates adequate security measures to mitigate risks such as unauthorised access to data, or 'hacking' of the device in order to communicate with the child (eg taking over microphone capabilities) or track their location.

Anticipate and provide for use by multiple users of different ages

If you provide a connected device then you need to pay attention to the potential for it to be used by multiple users of different ages. This is particularly the case for devices such as home hub interactive speaker devices which are likely to be used by multiple household members, including children, and may also be used by visitors to the home. Similarly

interactive toys are often shared or may be used by several children at once when they play together.

You can do this by a combination of:

- making sure that the service that you provide by default (the service that would be provided, for example, to occasional visitors to a household) is suitable for use by all children; and
- providing user profile options for people who use the device regularly (eg household members and frequent visitors to a household) to support use by adults, or to tailor the service to the age of a particular child.

Provide clear information about your use of personal data at point of purchase and on set-up

You should provide clear information indicating that the product processes personal data at the point of sale and prior to device set-up. Both the packaging of the physical product, and your product leaflet or instruction booklet (paper or digital) could carry a clear indication (such as an icon) that the product is 'connected' and processes users' personal data.

You should allow potential purchasers to view your privacy information, terms and conditions of use and other relevant information online without having to purchase and set up the device first, so that they can make an informed decision about whether or not to buy the device in the first place.

You should also have a particular focus on the tools you provide to facilitate the set-up of the connected toy or device. This is a key opportunity for you to provide information about how your service works, how personal data is used and to explain the implications of this, especially if set-up is activated using a screen-based interface. If the child's ongoing use of the device is not screen-based this is particularly important as this may limit the ways in which you can convey information to the child on an ongoing basis.

Find ways to communicate 'just in time' information

You should consider how your connected device operates and how best to communicate 'just in time' information to the child or their parent. (See the section of this code on transparency for more detail about 'just in time' notices.)

For example using auto-play audio messages, only allowing default settings to be changed via use of a support app, or facilitating interactive auto-bot 'conversations' with the user.

Avoid passive collection of personal data

You should provide features that make it clear to the child or their parent when you are collecting personal data. For example a light that switches on when the device is audio recording, filming or collecting personal data in another way.

If the device uses a stand-by or 'listening' mode (eg it listens out for the name you or the child has given to the device, or for another key word or phrase to be used, and activates data collection when that word or phrase is used) again you should provide a clear indication that listening mode is active. You should not collect personal data in listening mode.

You should provide features which allow collection or listening modes to be easily switched off on the device itself (a 'connection off' button), or via online functionality options, so that the toy or device can be used as a non-connected device so far as this is practicable.

Further reading outside the code

[Guide to the GDPR –Contracts and liabilities between controllers and processors](#)

[Guide to the GDPR – Security](#)

[Department for Digital, Culture, Media & Sport: Code of Practice for consumer IOT security](#)

15. Online tools

Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

What do you mean by ‘online tools’?

Online tools are mechanisms to help children exercise their rights simply and easily when they are online. They can be used to help children exercise their right to access a copy of their personal data, or to make a complaint or exercise any of their remedial rights.

Why is this important?

The GDPR gives data subjects the following rights over their personal data in articles 15 to 22:

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Recital 65 states that the right to erasure has particular relevance for children using online services:

“...that right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet...”

Article 12 of the GDPR provides that:

"12(1)The controller shall take appropriate measures to provide any communication under Articles 15 to 22 relating 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.....

(2)The controller shall facilitate the exercise of data subject rights under Articles 15 to 22.....

(3) The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by a further two months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject."

In order to comply with these provisions you need to find ways to make sure that children know about their rights and are able to easily exercise them. You have an obligation not just to allow children to exercise their rights but to help them to do so.

How can we make sure that we meet this standard?

In order for children to exercise their rights they firstly need to know that these rights exist and what they are.

Make your tools prominent

The tools which you provide to help children exercise their rights and report concerns to you must be easy for the child to find. You therefore need to give them prominence on your online service. You should highlight the reporting tool in your set up process and provide a clear and easily identifiable icon or other access mechanism in a prominent place on the screen display.

If your online service includes a physical product, for example a connected toy or speaker, you can include the icon on your packaging, highlighting online reporting tools as a product feature, and find ways to highlight reporting tools in a prominent way even if the product is not screen-based.

Make them age appropriate and easy to use

Your tools should be age appropriate and easy to use. You should therefore tailor them to the age of the child in question. The following table provides some guidelines. However, these are only a starting point and you are free to develop your own, service specific, user journeys that follow the principle in the headline standard.

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

Age range	Guidelines
0-5 Pre-literate & early literacy	<p>Provide icon(s), audio prompts or similar that even the youngest of children will recognise as meaning 'I'm not happy' or 'I need help'.</p> <p>If these buttons are pressed, or other prompts responded to, provide video or audio material prompting the child to get help from a parent or trusted adult.</p> <p>Provide online tools suitable for use by parents.</p>
6-9 Core primary school years	<p>Provide icon(s), audio prompts or similar that children will recognise as meaning 'I'm not happy' or 'I need help'.</p> <p>If these buttons are pressed, or other prompts responded to, provide video or audio material prompting the child to get help from a parent or trusted adult, then direct the child to your online tool.</p> <p>Provide online tools that children could use either by themselves or with the help of an adult.</p>
10-12 Transition years	<p>Provide icon(s), audio prompts or similar that children will recognise as meaning 'I'm not happy' or 'I need help'.</p>

	<p>If these buttons are pressed, or other prompts responded to, direct the child to your online tool and prompt them to get help from a parent or trusted adult if they need it.</p> <p>Provide online tools that children could use either by themselves or with the help of an adult.</p>
13 -15 Early teens	<p>Provide icon(s), audio prompts or similar that children will recognise as meaning 'I want to raise a concern' 'I want to access my information' or 'I need help'.</p> <p>If these buttons are pressed, or other prompts responded to, direct the child to your online tools and prompt them to get help from a parent or other trusted resource if they need it.</p> <p>Provide online tools suitable for use by the child without the help of an adult.</p>
16-17 Approaching adulthood	<p>Provide icon(s), audio prompts or similar that children will recognise as 'I want to raise a concern' 'I want to access my information' or 'I need help'.</p> <p>If these buttons are pressed, or other prompts responded to, direct the child to your online tools and prompt them to get help from a parent or other trusted resource if they need it.</p> <p>Provide online tools suitable for use by the child without the help of an adult.</p>

Make your tools specific to the rights they support

You should tailor your tools to support the rights children have under the GDPR. For example:

- a 'download all my data' tool to support the right of access, and right to data portability;
- a 'delete all my data' or 'select data for deletion' tool to support the right to erasure;

- a 'stop using my data' tool to support the rights to restrict or object to processing; and
- a 'correction' tool to support the right to rectification.

Used together with privacy setting such tools should help to give children control over their personal data.

Include mechanisms for tracking progress and communicating with you

Your online tools can include ways for the child or their parent to track the progress of their complaint or request, and communicate with you about what is happening.

You should provide information about your timescales for responding to requests from children to exercise their rights, and should deal with all requests within the timescales set out at Article 12(3) of the GDPR.

You should have mechanisms for children to indicate that they think their complaint or request is urgent and why, and you should actively consider any information they provide in this respect and prioritise accordingly. You should have procedures in place to take swift action where information is provided indicating there is an ongoing safeguarding issue.

Further reading outside this code

[Guide to the GDPR – individual rights](#)

Governance and accountability

At a glance

You should put systems in place to support and demonstrate your compliance with data protection legislation and conformance to this code. These should include implementing an accountability programme, having suitable data protection policies in place, providing appropriate training for your staff and keeping proper records of your processing activities.

In more detail

- [What do you mean by 'governance and accountability'?](#)
- [Why is it important?](#)
- [What do we need to do?](#)
- [What about certification schemes?](#)

What do you mean by 'governance and accountability'?

Governance and accountability means having systems in place to support and demonstrate compliance with data protection legislation and this code.

Why is it important?

It is important because it is a vehicle for you to build compliance as a long term sustainable activity across your business. It is a global concept which can work across jurisdictions and allow different approaches under different law to fit together. It is most successful when supported by Board level leadership.

Article 24(1) of the GDPR provides that:

“24(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Those measures shall be reviewed and updated where necessary.”

Article 5(2) of the GDPR says that you need to be able to demonstrate your compliance with the data protection principles:

“The controller shall be responsible for, and able to demonstrate compliance with paragraph 1 (accountability)”

What do we need to do?

Implement an accountability programme

You should implement an accountability programme to effectively address the standards in this code. This can be tailored to the size and resources of your business or organisation and the risks to children inherent in your online service. It should be driven by your DPO, if you have appointed one, and overseen by senior management at Board level if your business is structured in this way. For smaller businesses which may not have such formal structures it is still important to make sure that children's privacy is understood by key personnel and is seen as an important business priority and key accountability measure.

You should assess and revise the programme on an ongoing basis, building in changes to reflect the changing environment of children's privacy.

You should report against the standards in this code in any internal or external accountability reports, introducing KPIs (key performance indicators) on children's privacy to support this as appropriate.

Have policies to support and demonstrate your compliance with data protection legislation

You should have policies (proportionate to the size of your organisation) that document how your organisation ensures adherence to this code and

the requirements of the GDPR and PECR. For larger organisations these should include appropriate board level reporting mechanisms and mechanisms to ensure adequate resourcing of relevant projects.

In particular you should ensure that your policies cover your obligations under Article 30(1) to keep a record of your processing activities.

Train your staff in data protection

In order to meet the requirements of the GDPR, any staff involved in the design of your ISS need to understand what those requirements are and how we expect them to be met. So you should make sure that your staff receive appropriate training in data protection and are aware of the provisions of the GDPR and this code.

Keep proper records

Under Article 30(1) of the GDPR you are required to keep the following records of your processing activities:

- the name and contact details of your organisation (and where applicable, of other controllers, your representative and your DPO);
- the purposes of your processing;
- a description of the categories of individuals and categories of personal data;
- the categories of recipients of personal data;
- details of your transfers to third countries including documenting the transfer mechanism safeguards in place;
- retention schedules; and
- a description of your technical and organisational security measures.

In the context of providing an online service this rule applies to you regardless of the size of your organisation. This is because the Commissioner considers that, given the vulnerability of children and the risks inherent in them being online, any such processing is likely to result in a risk to the rights and freedoms of children.

There are templates on our website that you can use to record these details.

You should also keep a record of your DPIA. This is a key document that you can use to demonstrate that you have properly considered and

mitigated risks arising from your processing of children's personal data. It should help you to demonstrate your thinking and decisions on:

- whether children are likely to access your online service;
- what ages of children are likely to access your online service; and
- what measures you have taken to conform to this code.

Be prepared to demonstrate your conformance to this code

You should be prepared to demonstrate your conformance to this code to the ICO if we ask you to do so. You can do this by firstly providing us with copies of your DPIA, relevant policies, training records, and records of processing activities. You may also need to provide evidence of how you have implemented the provisions of the code in your online service in practice. For example, by showing us your privacy notices, or explaining or demonstrating your default settings, online tools, complaint processes and approach to profiling.

What about certification schemes?

Article 42 of the GDPR provides a mechanism for the establishment of certification and data protection seal schemes by which data controllers could demonstrate their compliance with the GDPR.

This would be of particular benefit to children and their parents in making decisions about which online services to use (or allow their children to use) without having to assess the compliance and practice of the online service provider themselves.

It would also benefit you as a provider of an online service to give assurance to your customers and potential customers of your data protection compliance, thereby increasing consumer confidence in online service and brand.

As and when any such schemes become available and offer certification of adherence to this code, you will be able to use them to demonstrate your compliance in accordance with article 24(1) of the GDPR.

Further reading outside this code

Guide to the GDPR Accountability and governance

[Documentation template for controllers](#)

[Documentation template for processors](#)

Enforcement of this code

At a glance

The ICO upholds information rights in the public interest. Data relating to children is afforded special protection in the GDPR and is a regulatory priority for the ICO. Conforming to the standards set out in this code will be a key measure of your compliance with data protection laws.

We will monitor conformance to this code through a series of proactive audits, will consider complaints, and take appropriate action to enforce the underlying data protection standards, subject to applicable law and in line with our Regulatory Action Policy. To ensure proportionate and effective regulation we will target our most significant powers, focusing on organisations and individuals suspected of repeated or wilful misconduct or serious failure to comply with the law. If you do not follow this code, you may find it difficult to demonstrate that your processing is fair and complies with the GDPR or PECR.

We have various powers to take action for a breach of the GDPR or PECR, including where a child's personal data has been processed in breach of relevant provisions of these laws. This includes the power to issue warnings, reprimands, stop-now orders and fines.

In more detail

- [What is the role of the ICO?](#)
- [How will the ICO monitor compliance?](#)
- [How will the ICO deal with complaints?](#)
- [What are the ICO's enforcement powers?](#)

What is the role of the ICO?

The Information Commissioner is the independent supervisory authority for data protection in the UK.

Our mission is to uphold information rights for the public in the digital age. Our vision for data protection is to increase the confidence that the public

have in organisations that process personal data. We offer advice and guidance, promote good practice, monitor and investigate breach reports, monitor compliance, conduct audits and advisory visits, consider complaints, and take enforcement action where appropriate. Our enforcement powers are set out in part 6 of the DPA 2018.

Our focus is on compliance with data protection legislation in the UK. In particular, to ensure that the protections provided for children's data are adhered to.

Where the provisions of this code overlap with other regulators we will work with them to ensure a consistent and co-ordinated response.

How will the ICO monitor conformance?

Key objectives in our Regulatory Action Policy include:

"To be proactive in identifying and mitigating new or emerging risks arising from technological and societal change" and,

"To be effective, proportionate, dissuasive and consistent in our application of sanctions, targeting our most significant powers (i) for organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data, and (ii) where formal regulatory action serves as an important deterrent to those who risk non-compliance with the law."

We have also made use of children's data a regulatory priority.

We will monitor conformance to this code using the full range of measures available to us from intelligence gathering through to using our audit or assessment powers to understand an issue, through to investigation and regulatory action where appropriate and proportionate..

Our approach is to encourage conformance. Where we find issues we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected. We will take account of the size and resources of the organisation concerned, the availability of technological solutions in the marketplace and the risks to children that are inherent in the processing. We will take a proportionate

and responsible approach, focussing on areas with the potential for most harm and selecting the most suitable regulatory tool.

How does the ICO deal with complaints?

If someone raises a concern with us about your conformance to this code or the way you have handled a child's personal data in the context of a relevant online service, we will record and consider their complaint.

We will take this code into account, along with other relevant legislation, when considering whether you have complied with the GDPR or PECR. In particular, we will take the code into account when considering questions of fairness, lawfulness, transparency and accountability.

We will assess your initial response to the complaint, and we may contact you to ask some questions and give you a further opportunity to explain your position. We may also ask for details of your policies and procedures, your DPIA, and other relevant documentation. However, we expect you to be accountable for how you meet your obligations under GDPR and PECR, so you should make sure that when you initially respond to complaints from individuals you do so with a full and detailed explanation about how you use their personal data and how you comply.

If we consider that you have failed (or are failing) to comply with the GDPR or PECR, we have the power to take enforcement action. This may require you to take steps to bring your operations into compliance or we may decide to fine you. Or both.

What are the ICO's enforcement powers?

We have various powers to take action for a breach of the GDPR or PECR, including where a child's personal data is involved. We have a statutory duty to take the provisions of this code into account when enforcing the GDPR and PECR.

Without prejudice to the specifics of applicable law such as the eCommerce Regulations 2002, 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 (or £17.5 million when

the UK GDPR comes into effect) or 4% of your annual worldwide turnover, whichever is higher.

In line with our policy, we consider that the public interest in protecting children online is a significant factor weighing in the balance when considering the type of regulatory action. This means that where we see harm or potential harm to children we will likely take more severe action against a company than would be the case for other types of personal data. We will nevertheless take account of the size and resources of the organisation concerned, the availability of technological solutions in the marketplace and the specific risks to children that are inherent in the processing. We will also take into account the efforts made to conform to the provision in this code.

Further reading outside this code[What we do](#)[Make a complaint](#)[What action can the ICO take to enforce PECR?](#)[Regulatory Action Policy](#)

Glossary

This glossary is included as a quick reference point for key data protection terms and abbreviations used in this code. It includes links to further reading and other resources which do not form part of this code, but may provide useful context and more detailed guidance.

ASA	The Advertising Standards Authority. See www.asa.org.uk
CAP code	The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing. See: www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html
Child	A person under the age of 18 years, as defined in the UNCRC.
Competent authority	A public authority listed in schedule 7 of the DPA 2018, or any other organisation or person with statutory law enforcement functions. For more information, see our separate Guide to Law Enforcement Processing .
Consent	A freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data. For more information, see our separate guidance on consent .
Controller	The person (usually an organisation) who decides how and why to collect and use the data. For more information, see our separate guidance on controllers and processors .
DPA 2018	The Data Protection Act 2018. For more information, see our separate introduction to data protection .
DPIA	Data protection impact assessment. For more information, see our separate guidance on DPIAs .
GDPR	The General Data Protection Regulation (EU) 2016/679 , as amended and incorporated into UK law. For more information, see our separate Guide to Data Protection . When the UK leaves the EU (or at the end of any agreed implementation period if we leave with a deal), you should read references to the GDPR in this code as references to the UK GDPR.

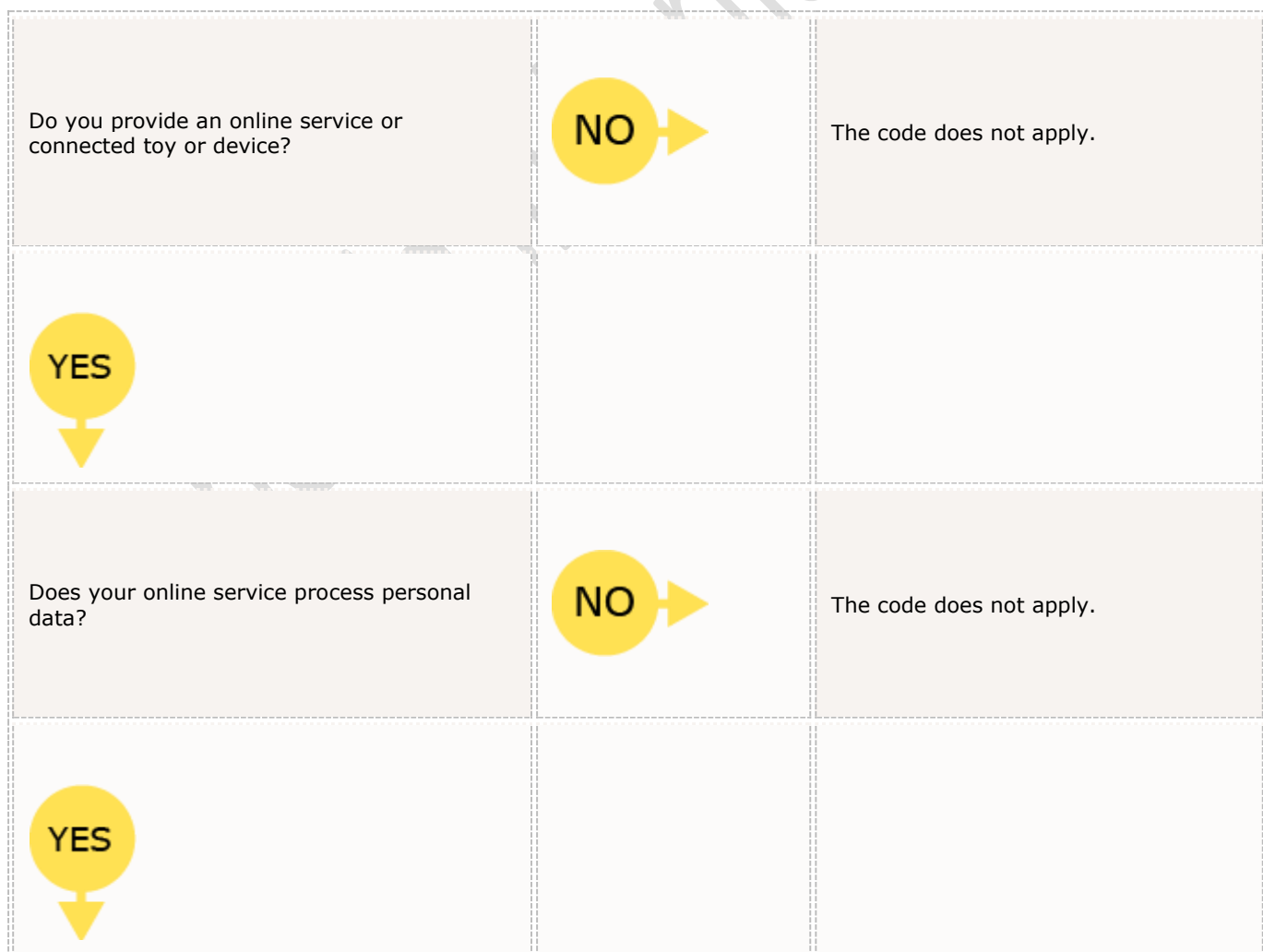
ISS	Information society service, as defined in Directive (EU) 2015/1535 and incorporated into the GDPR (any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient).
One-stop-shop	The one-stop-shop means you can generally deal with a single European supervisory authority taking action on behalf of the other European supervisory authorities. It avoids you having to deal with regulatory and enforcement action from every supervisory authority in every EEA and EU state where individuals are affected. For more information, see EDPB guidelines on the lead supervisory authority .
PECR	The Privacy and Electronic Communications (EC Directive) Regulations 2003. For more information, see our separate Guide to PECR .
PEGI	Pan European Game Information. For more information see www.pegi.info/
Processor	A person (usually an organisation) who processes personal data on behalf of a controller. For more information, see our separate guidance on controllers and processors.
UK GDPR	The UK version of the GDPR , as amended and incorporated into UK law after the UK leaves the EU by the European Union (Withdrawal) Act 2018 and associated Exit Regulations . The government has published a Keeling Schedule for the UK GDPR which shows the planned amendments.
UNCRC	The 1989 United Nations Convention on the Rights of the Child .

Annex A: Services covered by the code flowchart

This flowchart sets out the questions you will need to answer if you are uncertain whether your online service is covered by the code.

However, as a starting point, you should note that we expect the vast majority of online services used by children to be covered, and those that aren't covered to be exceptional.

The services that fall out of scope tend to do so for fairly technical legal reasons (such as the definition of an ISS as derived from Directive EU 2015/1535), so if you think you may be out of scope then you may benefit from getting your own legal advice to support or confirm this.



Is your online service a counselling or preventive service?	YES →	The code does not apply.
NO ↓		
Are you a law enforcement agency (eg police, courts) whose online service processes personal data for law enforcement purposes?	YES →	The code does not apply to any processing your online service does for law enforcement purposes. It may apply to any processing your online service does for other purposes.
NO ↓		
Is your online service the kind of service which is typically provided or funded on a commercial basis (even if the funding isn't provided by the end user)?	NO →	The code does not apply.
YES ↓		
Is your online service a 'general broadcast' service (a service which transmits radio or TV broadcasts to a general audience according to a set schedule or timetable)?	YES →	The code does not apply to your 'general broadcast' services. If you also provide 'on demand' broadcast services then the code may apply to these.
NO ↓		

Does your online service only provide information about a 'real-world' business (without allowing customers to buy products or access specific services online)?	YES →	The code does not apply.
NO ↓		
Is your service a 'traditional' voice telephony service as opposed to an internet based voice calling service or VOIP (Voice Over Internet Protocol)?	YES →	The code does not apply.
NO ↓		
Is your online service likely to be accessed by children? (This will depend upon whether the content and design of your service is likely to appeal to children, and any measures you may have in place to restrict or discourage their access to your service).	NO →	The code does not apply.
YES ↓		
Do you have an office, base, or other 'establishment' in the UK, and does your online service process personal data in the context of that establishment?	NO →	<p>The code applies to your service if it meets the following criteria:</p> <ul style="list-style-type: none"> • you offer your online service to UK users, or monitor the behaviour of UK users; and • (until the UK leaves the EU) you do not have an office base or other establishment elsewhere within the EEA (European Economic Area). <p>Otherwise the code does not apply.</p>
YES ↓		
The code applies to your service.		

Annex B: Age and developmental stages

Children are individuals, and age ranges are not a perfect guide to the interests, needs and evolving capacity of an individual child. However, 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, to help you assess what is appropriate for children of broadly that age.

This annex provides some guidance on key considerations relevant at different ages. This has been developed drawing on responses to the ICO's call for evidence on the age appropriate design code, ICO funded research by Sonia Livingstone at the London School of Economics and on the following sources:

- [UKCCIS report Education for a connected world](#)
- [UKCCIS report Children's online activities, risks and safety](#)
- [UKCCIS guide Child Safety Online](#)
- [Children's Commissioner for England report Life in Likes](#)
- [5Rights Foundation report Digital Childhood](#)
- [Revealing Reality report Towards a better digital future Informing the Age Appropriate Design Code](#)

Children with disabilities may have additional needs and you should consider any additional responsibilities you may have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

Age/Stage	key considerations
0-5 pre-literate and early literacy	<p>There is relatively little evidence on the understanding of the digital environment of children in this age range, particularly for 0-3 years old. However anecdotal evidence suggests that significant numbers of children are online from the earliest of ages and that any understanding and awareness of online risks that have children within this age range is very limited.</p> <p>At age 3-5 children start to develop the ability to 'put themselves in others shoes', but are easily fooled by appearances. They are developing friendships, although peer pressure is relatively low and parental or family guidance or influence is key. They are learning to follow clear and simple rules but are unlikely to have the cognitive ability to understand or follow more nuanced rules or</p>

	<p>instructions, or to make anything but the simplest of decisions. They have limited capacity for self-control or ability to manage their own time online. They are predominantly engaged in adult-guided activities, playing within 'walled' environments, or watching video streams.</p> <p>Children in this age range are less likely than older children to have their own device, although significant numbers do, and often play on their parents' devices which may or may not be set up with child specific profiles. They may use connected toys (such as talking teddies or dolls) and may also mimic parents' use of voice activated devices such as 'home hubs'.</p> <p>Children within this age range are pre-literate or in the earliest stages of literacy, so text based information is of very limited use in communicating with them.</p> <p>UK children in this age range cannot provide their own consent to the processing of their personal data in the context of an online service offered directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018). So if you wish to rely on consent as your lawful basis for processing their personal data you need parental consent.</p>
6-9 core primary school years	<p>Children in this age range are more likely than younger children to have their own device (such as a tablet), although use of parents' devices is still common. They are increasingly using devices independently, with or without the benefit of child specific profiles. Connected toys are popular and they may engage enthusiastically with voice activated devices such as home hubs.</p> <p>Children in this age range often prefer online gaming and creative based activities, and video streaming services remain popular. Children may be experimenting with social media use, either through social aspects of online games, through their parents' social media accounts or by setting up their own social media accounts. They may relate to and be influenced by online vloggers, particularly those within a similar age range.</p> <p>They are likely to be absorbing messages from school about online safety and the digital environment, and be</p>

	<p>developing a basic understanding of privacy concepts and some of the more obvious online risks. They are unlikely however to have a clear understanding of the many ways in which their personal data may be used or of any less direct or obvious risks that their online behaviour may expose them to.</p> <p>The need to fit in with their peer group becomes more important so they may be more susceptible to peer pressure. However home and family still tends to be the strongest influencer. They still tend to comply with clear messages or rules from home and school, but if risks aren't explained clearly then they may fill the gap with their own explanations or come up with protective strategies that aren't as effective as they think they are.</p> <p>Literacy levels can vary considerably and ability or willingness to engage with written materials cannot be assumed.</p> <p>UK children in this age range cannot provide their own consent to the processing of their personal data in the context of an online service offered directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018). So if you wish to rely on consent as your lawful basis for processing their personal data you need parental consent.</p>
10-12 transition years	<p>This is a key age range in which children's online activity is likely to change significantly. The transition, or anticipated transition, from primary school to high school means that children are much more likely to have their own personal device (pre-dominantly smartphones).</p> <p>There is also likely to be a shift towards use of the online environment to explore and develop self-identity and relationships, expand and stay in contact with their peer group, and 'fit in' socially. This may lead to an increased use of social networking functions or services by children within this age range, an increased susceptibility to peer pressure, branding and online 'influencers', and an increase in risk taking behaviours. Self-esteem may fall as children compare themselves to others and strive to present an acceptable version of themselves online and the 'fear of missing out' may become a concern.</p>

	<p>Online gaming and video and music streaming services are also popular. Children may feel pressurised into playing online games when their friends are playing, again for fear of missing out.</p> <p>Attitudes towards parental rules, authority and involvement in their online activity may vary considerably, with some children relatively accepting of this and others seeking higher levels of autonomy. However parents and family still tend to be the main source of influence for children in this age range.</p> <p>Children in this age range are moving towards more adult ways of thinking but may have limited capacity to think beyond immediate consequences, be particularly susceptible to reward based systems, and tend towards impulsive behaviours. Parental or other support therefore still tends to be needed, if not always desired. It may however need to be offered or encouraged in a less directive way than for younger children.</p> <p>Children in this age range are developing a better understanding of how the online environment operates, but are still unlikely to be aware of less obvious uses of their personal data.</p> <p>Although children in this age range are likely to have more developed literacy skills they may still prefer media such as video content instead.</p> <p>12 is the age at which, under s208 of the DPA 2018, children in Scotland are presumed (unless the contrary is shown) to be of sufficient age and maturity to have a general understanding of what it means to exercise their data protection rights. There is no such provision for children in the rest of the UK, although this may be considered a useful reference point.</p> <p>UK children in this age range cannot provide their own consent to the processing of their personal data in the context of an online service offered directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018).</p>
--	---

	So if you wish to rely on consent as your lawful basis for processing their personal data you need parental consent.
13-15 early teens	<p>In this age range the need for identification with their own peer group, and exploration of identity and relationships increases further and children are likely to seek greater levels of independence and autonomy. They may reject or distance themselves from the values of their parents or seek to actively flaunt parental or online rules. The use of new services that parents aren't aware of or don't use is popular as is the use of language that parents may not easily understand. However, despite this, family remains a key influence on children within this age range.</p> <p>The use of social media functions and applications is widespread although gaming and video and music streaming services are also popular. Again children may seek to emulate online 'influencers' or vloggers at this stage in their development.</p> <p>Children of this age may still look to parents to assist if they encounter problems online, but some may be reluctant to do so due to concerns about their parents' reaction to their online activity.</p> <p>Developmentally they may tend toward idealised or polarised thinking and be susceptible to negative comparison of themselves with others. They may overestimate their own ability to cope with risks and challenges arising from online behaviour and relationships and may benefit from signposting towards sources of support, including but not limited to parental support.</p> <p>Literacy skills are likely to be more developed but they may still benefit from a choice of media.</p> <p>13 is the age at which children in the UK are able to provide their own consent to processing, if you relying on consent as your lawful basis for processing in the context of offering an online service directly to a child (by virtue of Article 8(1) of the GDPR and s9 of the DPA 2018).</p>

<p>16-17 approaching adulthood</p>	<p>By this age many children have developed reasonably robust online skills, coping strategies and resilience. However they are still developing cognitively and emotionally and should not be expected to have the same resilience, experience or appreciation of the long term consequences of their online actions as adults may have.</p> <p>Technical knowledge and capabilities may be better developed than their emotional literacy or their ability to handle complex personal relationships. Their capacity to engage in long term thinking is still developing and they may still tend towards risk taking or impulsive behaviours and be susceptible to reward based systems.</p> <p>Parental support is more likely to be viewed as one option that they may or may not wish to use, rather than as the preferred or only option, and they expect a reasonable level of autonomy. Signposting to other sources of support in addition to parental support is important.</p> <p>By virtue of Article 8(1) of the GDPR and s9 of the DPA 2018, if you are relying on consent as your lawful basis for processing in the context of offering an online service directly to a child, UK children in this age range can provide their own consent to the processing of their personal data.</p>
--	---

Annex C: Lawful basis for processing

The guidance in this annex is not linked to a specific standard in the code, but if you provide an online service to children it will help you comply with your lawfulness obligations under the GDPR and DPA 2018.

- [What is a lawful basis for processing?](#)
- [Which lawful basis can we use for our 'core' processing?](#)
- [Which lawful basis can we use for 'non-core' processing?](#)
- [When do we have to get parental consent?](#)
- [What about special category data?](#)

What is a lawful basis for processing?

You must have a valid lawful basis for each of your processing activities. Article 6 of the GDPR sets out six potential lawful bases:

- (a) **Consent:** the individual has given valid consent for you to process their personal data for a specific purpose.
- (b) **Contract:** the processing is necessary to perform a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) **Vital interests:** the processing is necessary to protect someone's life.
- (e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests – in particular where they are a child. (This cannot apply if you are a public authority performing your official tasks.)

It is up to you to decide which lawful basis for processing is most appropriate to your processing, and demonstrate that it applies. This depends on your specific purposes and on the context of the processing. In

practice it is likely that you will have more than one purpose, in which case you may have more than one basis for processing.

You should consider this separately for each distinct processing activity, thinking about what you want to do with the personal data you are collecting and why, and taking into account how essential this is to the provision of your online service.

Further reading outside this code:[Lawful basis for processing](#)[Lawful basis interactive guidance tool](#)

Which lawful basis can we use for our ‘core’ processing?

By ‘core processing’, we mean processing which is integral to the provision of your core service – in other words, you need to process the data in that way in order to actually deliver the elements of the service the individual has signed up for. This doesn’t include processing for broader business purposes (eg for marketing, service improvement or as part of an indirect funding model).

For this type of core processing, you could consider:

- **(b) Contract:** the most obvious basis is ‘necessary for performance of a contract’. However, if you want to rely on this basis, you need to be sure that the child has the legal capacity to enter into a contract. If the child is not competent to enter into the contract then the contract is voidable. If the contract is voided then this basis for processing will not be valid.
- **(f) Legitimate interests:** alternatively you can consider legitimate interests (unless you are a public authority performing your functions). If you do choose to rely on legitimate interests, you have a particular responsibility to protect children from risks that they may not fully appreciate and from consequences that they may not envisage. You must ensure their interests are adequately protected and that there are appropriate safeguards. You need to give extra weight to their interests, and you need a more compelling interest to justify any potential impact on children. Your DPIA is a useful tool to help you assess this balance.
- **(e) Public task:** if you are offering a service as part of your public functions, or performing a specific task in the public interest. You need to identify a statutory or common law basis for that function or task.

Consent is unlikely to be the most appropriate basis for processing which is necessary to deliver the core service. This is because the processing is a condition of the contract, so asking for separate consent is unnecessary and potentially confusing. It risks diluting the general concept of consent as a clear and separate choice with no strings attached, and may contribute to 'consent fatigue'. You only need consent where specifically required under another provision, such as:

- to comply with PECR rules - although you don't need consent for cookies which are strictly necessary for your service; or
- to get explicit consent for specific elements of your service that process special category data (more on this below).

Legal obligation may be relevant for some fraud prevention, child protection or safeguarding measures, if you can point to a specific legal provision or appropriate source of advice or guidance on your legal obligations.

Vital interests is unlikely to be relevant in this context. Legitimate interests is likely to be a more reliable basis for any measures you take to protect a child's health or safety.

Which lawful basis can we use for 'non-core' processing?

By 'non-core' processing, we mean processing that is not integral to the provision of your core service. This includes processing for optional elements of the service, or processing for broader business purposes such as marketing, service improvement or indirect funding models.

You should give the child (and their parent where appropriate) as much choice as you can over these elements of your processing. This includes as a minimum implementing the standards in this code on default privacy settings, data minimisation, geolocation and profiling.

For optional elements of your service which a child has specifically activated, you can consider **necessary for contract** for any processing which is objectively necessary to deliver that specific element of the service if the child has capacity to enter into a contract, in the same way as for core processing. You can also consider **legitimate interests**. However, for these to apply, you must give the child separate choices to activate each separate element of the service wherever this is functionally possible. You cannot

bundle independent elements of a service together. See also the [standard on data minimisation in this code](#).

You do not need consent under PECR cookie rules as long as the processing is strictly necessary for these extra elements of a service, and they have been requested by the child. There are advantages to using legitimate interests or contract instead of consent, to avoid repeated consent requests and 'consent fatigue'. However, you still need to conform to the standards in this code related to privacy settings and controls, even if this falls short of a full consent mechanism.

To reinforce the importance of a child's choice, or as a safeguard against a particular risk to a child's interests, you may decide to rely on **consent** for some non-core processing. If you do so then you need to ensure you use a positive opt-in method of consent which is clear, separate from your terms and conditions, separate from your privacy information, and easy to withdraw. You must also comply with Article 8 of the GDPR (as adapted by section 9 of the DPA 2018) and obtain parental consent for children under 13. More on this below. You must also still conform to all the standards in this code to the extent they are relevant to your service.

You should remember that you need GDPR-compliant consent under PECR for any relevant cookies, apps or other technologies which gain access to, or store data on, the user device, but which are not strictly necessary for the service. You should also note the opinion of the European Data Protection Board (EDPB) about processing for the purposes of online behavioural advertising. EDPB has been clear that it considers that legitimate interests will not be an appropriate lawful basis for processing for this type of online activity (which leaves consent as the only remaining viable lawful basis for processing).

If you're processing for broader business purposes and you are not caught by the cookie rules, you may still be able to consider legitimate interests, public task or legal obligation, depending on why and how you are using the data.

Further reading outside this code:

See our separate guidance on:

[Consent](#)

[Contract](#)

[Legal obligation](#)

[Public task](#)

[Legitimate interests](#)

[Guide to PECR – Cookies and similar technologies](#)

Further reading - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB has published '[Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR](#)'. This provides useful information about how the cookie rules relate to the GDPR and re-states the positions previously taken by WP29 about when consent should be required for certain processing operations beyond the setting of cookies.

WP29 previously published '[Opinion 3/2013 on purpose limitation](#)' and '[Opinion 6/2014 on the notion of legitimate interests](#)'. Although this guidance was produced under the previous data protection framework, much of it applies under the GDPR.

When do we have to get parental consent?

Article 8(1) of the GDPR (as modified by section 9 of the DPA 2018) says that if you are relying on consent as your lawful basis:

Quote

"in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least [13] years old. Where the child is below the age of [13] years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

This does not mean that you always have to obtain parental consent for users under 13. It only applies if you make your service available to children, and you rely on consent as your lawful basis (eg for any non-core processing, cookies or similar technologies, or processing of special category data).

If so, it says you need to make 'reasonable efforts' to obtain and verify parental consent for children under 13.

You can take available technology into account in deciding what is reasonable for the purposes of Article 8. You can also consider other circumstances, including your resources and the level of risk identified in your DPIA, but you must be able to justify your approach.

Meeting the standards in this code should also help. This is because the standards in the code work together to mitigate risks arising from the processing of children's personal data. In particular, if you conform to the standard on age appropriate application (and apply the standards to all users where you are unable to establish age with a level of confidence that is appropriate to the risks) then you are providing significant protections for children by default, even if they have lied about their age. This means that the risks that might arise from not knowing how old a user is, or from not verifying parental consent to a high standard, are reduced. Parental consent becomes only one of a number of measures in place to protect children online.

Your approach to age verification and parental consent under Article 8 should therefore be compatible with your approach to age appropriate application under this code.

If you verify age and parental authority for Article 8 purposes then you need to do so in a privacy-friendly way. Collect the minimum amount of 'hard identifiers' (such as passport scans or credit card details). Remember that you need to comply with the GDPR in your processing of any personal data you collect for verification purposes, including the purpose limitation, data minimisation, storage limitation and security principles.

If you are using a third party verification service, you should use 'attribute' systems which offer a yes/no response when asked if an individual is over a given age, or if a person holds parental responsibility over the child.

If you can show that your processing is particularly low-impact and does not carry any significant risk to children, you may be able to show that self-declaration mechanisms are reasonable on their own (eg analytics cookies).

If the risks are higher then you need to either rely on more robust methods, or mitigate risks by applying the standards in this code to all users regardless of their self-declared age.

Further reading outside this code:[Detailed guidance on consent](#)[Children and the GDPR – What are the rules about an ISS and consent?](#)

What about special category data?

If your online service processes any special category data of children, you must identify both a lawful basis under Article 6 **and** an additional condition for processing that data under Article 9. Special category data includes information about:

- race;
- ethnic origin;
- politics
- religion;
- trade union membership;
- genetics;
- biometric identification (eg facial or fingerprint recognition);
- health (including data collected by fitness apps);
- sex life; or
- sexual orientation.

The most relevant Article 9 conditions are likely to be:

- **Article 9(2)(a) - explicit consent:** If you need to process special category data to provide a service to the individual, explicit consent may be available as your condition for processing that data even if it is a condition of service. However, you must be confident that you can demonstrate that consent is still freely given. In particular, that the processing is objectively necessary to perform a requested element of the service, and not bundled together with other elements of the service or included in your terms for broader business purposes.
- **Article 9(2)(d) - not-for-profit bodies:** if you are a not-for-profit body and your online service has a political, philosophical, religious or trade union aim. The child must either be a member or someone in regular contact with you for those purposes, and you must not disclose their data outside your organisation without consent. You must also comply with all the safeguards set out in this code, as well as other appropriate safeguards identified in your DPIA.
- **Article 9(2)(g) - substantial public interest:** you can rely on this condition if you can meet one of 23 specific substantial public interest conditions set out in schedule 1 of the DPA 2018. You also need an 'appropriate policy document' which briefly sets out which condition you

are relying on, how you comply with the principles, and your retention and deletion policies (this can be taken from step 4 of your DPIA).

In particular, you may be able to consider the specific substantial public interest conditions in schedule 1 of the DPA 2018 for:

- statutory or government purposes (condition 6);
- preventing or detecting unlawful acts (condition 10);
- preventing fraud (condition 14); or
- safeguarding of children (condition 18).

You should review the detail of these conditions carefully. If no other specific condition is available, you must get the valid explicit consent of the child (or their parent, if the child is under 13), otherwise you cannot process special category data.

You must document and justify your condition as part of your DPIA.

Further reading outside this code

See our separate guidance on [special category data](#)

[See our separate detailed guidance on consent](#)

Annex D: DPIA template

This template is an example of how you can record your DPIA process and outcome for an online service likely to be accessed by children. It is adapted from our general DPIA template, and follows the process set out in our DPIA guidance and the age appropriate design code. It should be read alongside the code and DPIA guidance, and the [Criteria for an acceptable DPIA](#) set out in European guidelines.

You should start to fill out the template early in the design of your online service, or early in your development process if you are making a significant change to an existing online service likely to be accessed by children. The final outcomes should be integrated back into the design of your service.

Submitting controller details

Name of controller	
Subject/title of DPIA	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly the nature of your online service, and the current stage of design or development. You may find it helpful to refer or link to other documents. Summarise when and how you identified the need for a DPIA.

To be laid in Parliament

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What are the sources of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? Does your service involve any profiling, automated decision-making, or geolocation elements? What are your plans (if any) for age-assurance? What are your plans (if any) for parental controls?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your service? Are you designing it for children? If not, are children under 18 likely to access it anyway? What is the likely age range of your users? How much control will they have? Would they understand and expect you to use their data in this way? Does your service use any nudge techniques? Are there prior concerns over similar services or particular security flaws? Is your service novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in, particularly over online risks to children? Are there any relevant industry standards, codes of practice or public guidance in this area? What responsibilities do you have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland. Is there any relevant guidance or research on the development needs, wellbeing or capacity of children in the relevant age range? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve with your service? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? What are the specific intended benefits for children?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – and specifically how you will seek the views of children and parents – or justify why it's not possible to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult experts in children's rights and developmental needs? If not, why not? Do you plan to consult any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? If you use AI, how will you avoid bias and explain its use? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Describe how you comply with the age-appropriate design code: what specific measures have you taken to meet each of the standards in the code?

- 1. Best interests of the child:**
- 2. Data protection Impact Assessments:**
- 3. Ageappropriate application:**
- 4. Transparency:**
- 5. Detrimental use of data:**
- 6. Policies and community standards:**
- 7. Default settings:**

8. Data Minimisation:

9. Data sharing:

10. Geolocation:

11. Parental controls:

12. Profiling:

13. Nudge techniques:

14. Connected toys and devices:

15. Online tools:

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include as a minimum an assessment of particular risks to children as listed in the DPIA standard in the age appropriate design code. You may need to consider separately for different age groups.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Describe source of risk and nature of potential impact on individuals. Include as a minimum an assessment of particular risks to children as listed in the DPIA standard in the age appropriate design code. You may need to consider separately for different age groups.	Likelihood of harm	Severity of harm	Overall risk

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

If you would like to contact us please call 0303 123 1113

ico.org.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF