Age appropriate design: a code of practice for online services

Consultation document

ico.
Information Commissioner's Office

Contents

Foreword

An introduction by Information Commissioner Elizabeth Denham will be included in the final version of the Code.

Summary of code standards

This code contains practical guidance on 16 standards of age-appropriate design for information society services likely to be accessed by children:

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. **Age-appropriate application:** Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

3. **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.

4. **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.

5. **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).

6. **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).

7. **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.

8. **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.

9. **Geolocation:** Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, 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 must default back to off at the end of each session.

10. **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.

11. **Profiling:** Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, 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).

12. **Nudge techniques:** Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use.

13. **Connected toys and devices:** If you provide a connected toy or device ensure you include effective tools to enable compliance with this code.

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

15. **Data protection impact assessments:** Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

16. **Governance and accountability:** Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code.

About this code

At a glance

This code provides practical guidance about 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 difficult to demonstrate your compliance, should we take regulatory action against you.

In more detail

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 provides practical guidance on 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 takes account of the standards and principles set out in the United Nations Convention on the Rights of the Child (UNCRC), and sets out

specific protections for children's personal data in compliance with the provisions of the General Data Protection Regulation (GDPR).

If you provide relevant online services, this code will help you to comply, and demonstrate that you comply, with your data protection obligations. Compliance with 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 those services to take responsibility for ensuring that their services are appropriate to the child's age, take account of their best interests, and respect 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 under 18, 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).

Annex B 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.

The Privacy and Electronic Communications Regulations (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.

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].

If you fail to act in accordance with a provision of this code you may invite regulatory action and you will find it difficult to demonstrate compliance with the law. 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 comply with the code?

If you don't comply with the code, you are likely to find it 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 this code and 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 or 4% of your annual worldwide turnover, whichever is higher.

For more information, see the separate section on enforcement of this code.

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).

However, 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.

How should we use the code?

The summary at the start of this code lists the 16 headline 'standards of age-appropriate design'. The main body of this code is then divided into 16 sections, each giving more detailed guidance on what the standard means, why it is important, and how you can implement it in practice.

Although the summary gives you an overview of the measures you need to implement, you need to read the code in full to ensure you understand and implement each standard properly. These standards are cumulative and interdependent - you must implement all of them in order to demonstrate your compliance with 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 service is appropriate for children who are likely to access it, 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 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

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?

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

> "relevant information society services which are likely to be accessed by children."

'Relevant' ISS are those which involve the processing of personal data to which the GDPR applies.

What do you mean by an 'information society service'?

'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 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. It does not cover public authorities providing other types of direct public services online (as these are not normally provided for remuneration).

If you are a small business with a website, your website will only be 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. However, you must still comply with the GPDR and PECR.

If you are uncertain whether your service is an ISS or not then we recommend you take your own legal advice.

What types of online services are not covered by the code?

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. An online booking service for an in-person appointment does not qualify as an ISS.

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). It also does not include telephony services including VOIP (internet calling) 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. However, more general health, fitness or wellbeing apps or services are covered.

This code only applies to online services which are covered by the GDPR. It does not apply to any online services provided by a police force or other competent authority for law enforcement purposes.

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 children 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.

This means that when you design your service you need to think about whether it (or any element of it) is likely to appeal to, and therefore be accessed by, children, even if this is not your intent. If it is likely to be accessed by children, then it will be covered by the code. You may need to carry out some market research, or refer to current evidence on user behaviour and the user base of existing services and service types.

If you believe only adults are likely to use your service so that this code does not apply, you need to be able to demonstrate that this is in fact the case. You may be able to rely on market research, the nature and context of the service, or specific measures you have taken to limit access by children. The important point is that even if the service is aimed at adults, you must be able to point to specific documented evidence to demonstrate that children are not likely to access the service in practice.

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 – even if this is only a small proportion of your overall user base - you need to comply with the code.

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.

Under the GDPR one-stop-shop arrangements, if you have a lead supervisory authority other than the ICO and you do not have a UK establishment, this code will not apply.

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
Recital 18 of the Directive on electronic commerce 2000/31/EC
Ker-Optika v ANTSZ (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

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."

This part of the code gives detailed guidance on each of the 16 standards of age-appropriate design. You need to read the code in its entirety to fully understand and properly implement these standards. The standards are cumulative and interdependent - you must implement all of them in order to demonstrate your compliance with the code.

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. To be effective, you need to design these measures in, not bolt them on.

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 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:

"5. [Countries] shall respect the responsibilities, rights and duties of parents or, where applicable the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention"

"14.2 [Countries] shall respect the rights and duties of the parents and, when applicable, legal guardians, to provide direction to the child in the

exercise of his or her right in a manner consistent with the evolving capacities of the child"

"18.1 [Countries] shall use their best efforts to ensure recognition of the principle that both parents have common responsibilities for the upbringing and development of the child. Parents or, as the case may be, legal guardians, have the primary responsibility for the upbringing and development of the child. The best interests of the child will be their basic concern."

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:

"12. [Countries] shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child."

"13.1 The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice."

"14.1 [Countries] shall respect the right of the child to freedom of thought, conscience and religion."

"15.1 [Countries] recognize the rights of the child to freedom of association and to freedom of peaceful assembly"

"16.1 No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
16.2 The child has the right to the protection of the law against such interference or attacks."

"17. [Countries] recognize the important function performed by the mass media and shall ensure that the child has access to information from a diversity of national and international sources, especially those aimed at the promotion of his or her moral well-being and physical and mental health."

"31.1 [Countries] recognize the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts"

"32.1 [Countries] States Parties recognize the right of the child to be protected from economic exploitation and from performing any work that is likely to be hazardous or to interfere with the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral or social development.

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.

Although as a provider of online service you may not be directly subject to the UNCRC, 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.

What do we need to do to 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. 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 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;
- 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. Age-appropriate application

Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish children from adults.

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 protected. If your service is likely to be accessed by children but you don't know which users are children, you must apply the code to all users.

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. To achieve this aim, the standards must:

- apply to all children using those services; and
- take account of the age and development needs of those children, to ensure appropriate protection for children of all ages.

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 an individual 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

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

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. See Annex B for full details.

What do we need to do to meet this standard?

Apply the standards in this code to all children

You should ensure that you apply the standards in this code to all children using your service. This means you must apply these standards to all users unless you have robust age checks in place to distinguish children from adults. Asking users to self-declare their age or age range does not in itself amount to a robust age-verification mechanism under this code.

In practice, you can choose whether to apply the standards in this code to:

- all users;

- all users by default, but offer robust age-verification mechanisms to allow adults who can prove their age to opt out of some or all of those safeguards; or

- only users who are children (and not to users who are adults), if you use robust age-verification mechanisms upfront to confirm the age of each user.

We recommend that you give your users a choice over the use of age verification wherever possible. In other words, we recommend that you provide a child-appropriate service to all users by default, with the option of age-verification mechanisms to allow adults to opt out of the protections in this code and activate more privacy-intrusive options if they wish.

This approach limits age barriers and incentives for children to lie about their age, limits the collection of hard identifiers, helps demonstrate privacy by design and default for all users, and respects the autonomy of adult users to make their own choices. It also recognises that some children do not have access to 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.

If you believe only adults are likely to access your service so that this code does not apply, you need to be able to demonstrate that this is in fact the case. If you have robust age-verification in place, that will provide the clearest evidence, but you may also be able to rely on other documented evidence that children are not likely to access the service. For more information, see the section on services covered by this code.

If you use age-verification, make it robust and privacy-friendly

If you do use age-verification to allow you to tailor your service to adults without regard to this code, make sure the mechanism you use is robust and effective. You must be able to demonstrate that children cannot easily circumvent the age checks.

You may be able to collect and record personal data which provides proof of age yourself. If so, remember that you need to comply with data protection obligations in relation to your collection and retention of that data, including data minimisation, purpose limitation, storage limitation and security obligations. You must not use data collected for age-verification purposes for any other purpose.

Alternatively, you could consider using a trusted third-party age-verification service. This allows you to reduce the amount of personal data you collect, and take advantage of technological expertise and developments in the

field. If you do use a third party service, you need to carry out some due diligence to satisfy yourself that their mechanism is suitably robust and compliant with data protection standards, and provide your users with clear information about the service you use.

Age-verification 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 robust age-verification services which comply with data protection standards.

Tailor the measures in this code to the age range of your users

You need to take account of the information you have about the age of a child when applying the standards in this code, even if you don't use age-verification. You can choose your approach to identifying the age of the child for these purposes:

- Ask users to self-select their age range. This is not age verification, but allows you to tailor the experience to the declared age of the child to some extent (eg to meet transparency standards). However, you must ensure the service applies all the safeguards in this code and takes account of the best interests of children of all ages, irrespective of the declared age of the user.

- Rely on use of the service itself to demonstrate the appropriate age range (or equivalent developmental stage) of users. This will only be appropriate if your service is specifically designed only for children of a particular age, and you can show that it is unlikely to be accessed by children at another stage of development (eg online services aimed at pre-literate children, or early readers). This allows you to fully tailor the experience to the age range of the target group when applying the standards in this code, as the risk to other children will be minimal.

- Use robust age-verification measures. You do not have to use age-verification, but this option allows you to give adult users more choices which may not comply with this code. It also allows you more scope to tailor your service to children of different ages, while still avoiding specific risks to children in other age ranges.

Tailoring your services to the age of the child does not mean you need less protection for older children. It means that you may need to apply different

measures for different age groups in order to meet the standards in this code. More specific information on age-appropriate factors to consider when applying the standards is included in the detailed guidance on each standard, where relevant, but for example you should consider:

- **Best interests of the child:** the best interests of the child will depend on their evolving capacity and development needs. You need to take account of the different needs of different age ranges when designing your service.

- **Transparency:** develop different levels of information explaining your service, aimed at and appropriate for the different age ranges using your service. You should then tailor the information you provide to each user to the declared age of that user.

- **Default settings:** take account of the different needs of different age ranges when developing prompts and other safeguards to mitigate the risks of activating extra elements of the service or changing default settings.

- **Parental controls:** develop information appropriate for different age ranges to ensure children are aware when parental monitoring is switched on. You should then tailor the information you provide to the declared age of each user.

- **Profiling:** take account of the different needs of different age ranges when assessing the risks and benefits of profiling. You should consider the declared age of your user to help ensure you don’t feed them inappropriate content for their age range.

- **Detrimental use of data:** tailor your use of data to the declared age of the user, if there is relevant age-specific advice.

- **Online tools:** develop online reporting tools that are appropriate for different age ranges. You should then tailor the version of the tools you offer to the declared age of the user.

- **DPIAs:** consider the needs of different age ranges when assessing the risk of your service, and identifying appropriate measures to mitigate those risks. If you identify a high risk from a particular element of your service or to a particular age-group, you can consider implementing

robust age-verification for that element, as one potential mitigating measure.

3. 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.

What do we need to do to meet this standard?

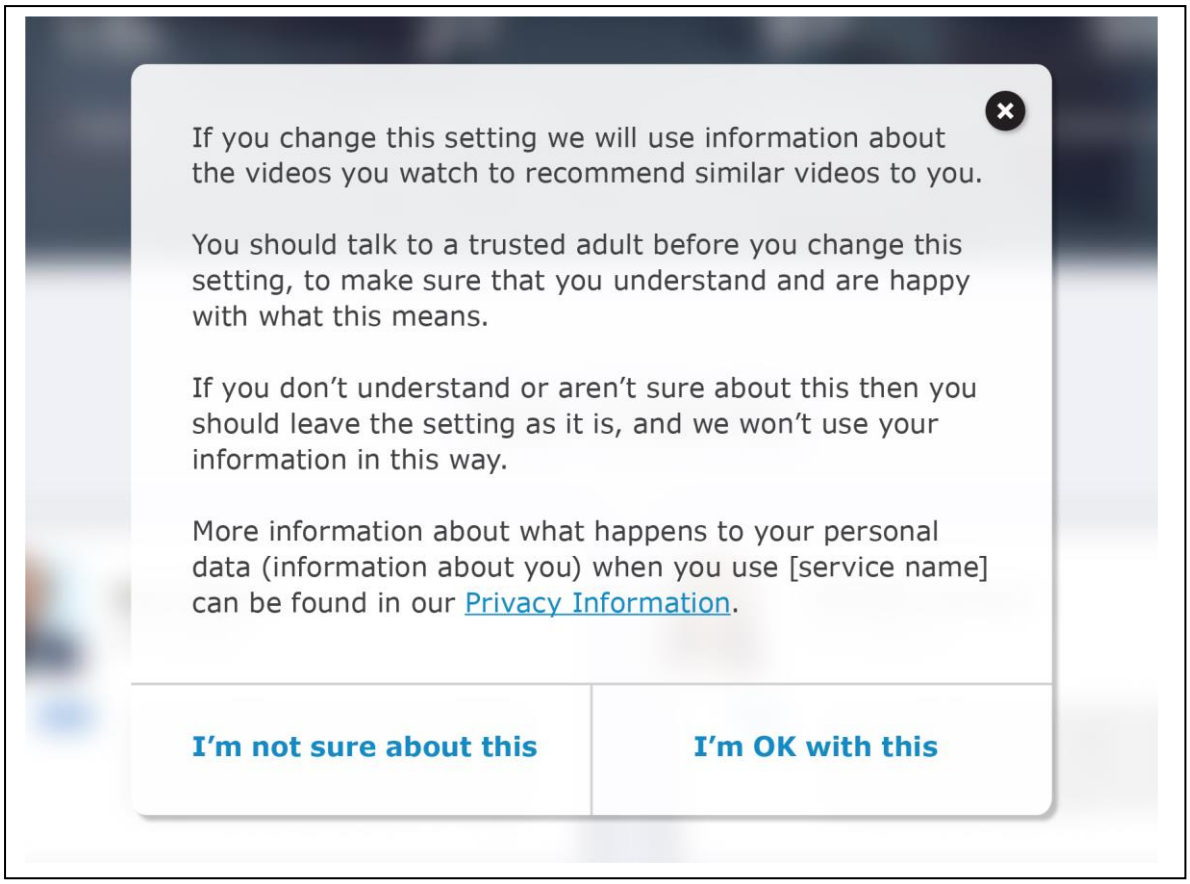
Provide clear privacy information

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 upon 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 upon the age of the child, 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 of your user journey at which 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 will need to 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 upon written communications.

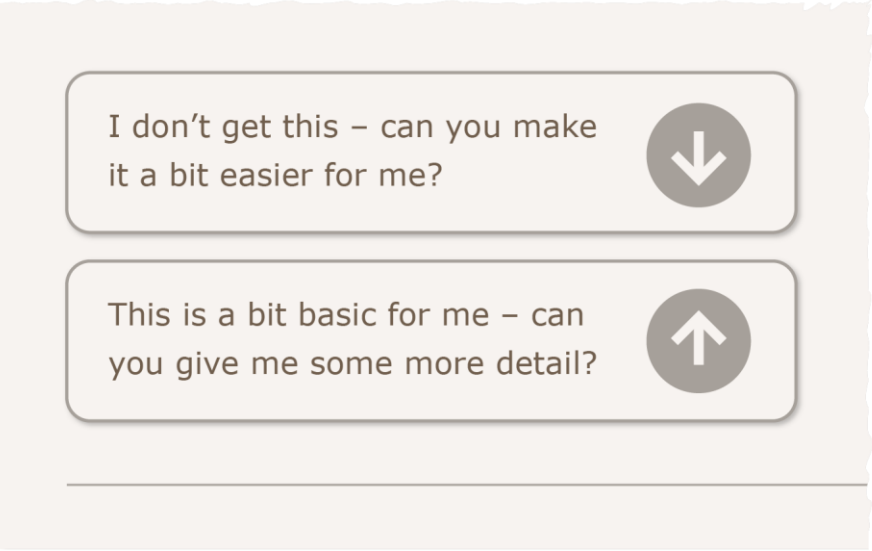
You may use tools such as privacy dashboards, layered information, icons and symbols to aid children's understanding and to present the information in a child friendly way. You should consider the modality of your service, and take into account user interaction patterns that do not take place in screen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

Tailor your information to the age of the child

You should tailor the content and presentation of the information you provide to the age of the child accessing the service. For younger children, with more limited levels of understanding, you may need to provide less detailed information for the child themselves and rely more upon 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 always provide 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 upon their individual level of understanding.



The following table provides some guidelines. However, they are only a starting point and you should 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 your user testing in your DPIA to support your final conclusions and justify the presentation and content of your final resources.

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

Age range	Guidelines
0-5 Pre-literate & early literacy	Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents. Provide audio or video prompts telling children to leave things are as they are or get help from a parent or trusted adult if they try and change any high privacy default settings.
6-9 Core primary school years	Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents. Provide cartoon, video or audio materials to sit alongside parental resources. Explain the basic concepts of online

	privacy within your service, the privacy settings you offer, who can see what, their information rights, how to be in control of their own information, and respecting other people's privacy. Explain the basics of your service and how it works, what they can expect from you and what you expect from them. Provide resources for parents to use with their children to explain privacy concepts and risks within your service. Provide resources for parents to use with their children to explain the basics of your service and how it works, what they can expect from you and what you expect from them. If a child attempts to change a default high privacy setting provide cartoon, video or audio materials to explain what will happen to their information and any associated risks. Tell them to leave things as they are or get help from a parent or trusted adult before they change the setting.
10-12 Transition years	Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for parents. Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for children within this age group. Allow children to choose between written and video/audio options. Give children the choice to upscale or downscale the information they see (to materials developed for an older or younger age group) depending upon their individual needs. If a child attempts to change a default high privacy setting provide written, cartoon, video or audio materials to explain what will happen to their information and any associated risks. Tell them to leave things as they are or get help from a parent or trusted adult before they change the setting.
13 -15 Early teens	Provide full privacy information as required by Articles 13 & 14 of the GDPR in a format suitable for this age group. Allow them to choose between written and video/audio options. Give them the choice to upscale or downscale the

	information they see (to materials developed for an older or younger age group) depending upon their individual needs. If a child attempts to change a default high privacy setting provide written, video or audio materials to explain what will happen to their information and any associated risks. Prompt them to ask for help from a parent or trusted adult and not change the setting if they have any concerns or don't understand what you have told them. Provide full information in a format suitable for parents to sit alongside the child focused information.
16-17 Approaching adulthood	Provide full information in a format suitable for this age group. Allow them to choose between written and video/audio options. Give them the choice to upscale or downscale the information they see (to materials developed for an older or younger age group) depending upon their individual needs. If a child in this age group attempts to change a default high privacy setting provide written, video or audio materials to explain what will happen to their information and any associated risks. Prompt them to check with an adult or other source of trusted information and not change the setting if they have any concerns or don't understand what you have told them. Provide full information in a format suitable for parents to sit alongside the child focused information.

Further reading outside this code
Guide to the GDPR – lawfulness, fairness and transparency
Guide to the GDPR – the right to be informed

4. 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 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.

What do we need to do to 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.

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.

Where evidence is contradictory or inconclusive and no formal Government position has been reached then, in order to take account of the best interests of the child, you should apply a pre-cautionary approach. This means that 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 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.

Strategies used to extend user engagement

Strategies used to extend user engagement, sometimes referred to as 'sticky' features 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 upon 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.'

Until such time as a formal position is adopted you should therefore not use children's personal data to support these types of mechanisms and strategies. You should also 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

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'

5. 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.

What do we have to do to meet this standard?

To some extent this will depend upon 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 those 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 upon '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 in place to properly uphold your own user behaviour policies then your original collection and continued use of 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 adequate systems in place 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 in place to ensure that it is. If you say that you will not tolerate bullying then you need to have adequate mechanisms in place 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 upon the age of your users then you need to take account of the age of the child when upholding your policies.

6. 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 in which you can 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?

They are 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 use them to support the exercise of children's data protection rights (such as the rights to object to or restrict processing). They can also 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

What do we need to do to meet this standard?

Provide 'high privacy' default settings

Your default position for each individual privacy setting should be privacy enhancing or 'high privacy'.

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

This will also mean 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, more intrusive, uses of personal data, including any uses designed to personalise the service have to be individually selected and activated by the child (assuming that it is appropriate to allow the setting to be changed).

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 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 upon your assessment of the risks inherent in the processing covered by each setting and could include age verification. 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 geo-location data.

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, for example 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 (for

example 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, so 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.

Reset defaults to high privacy for existing users

You should reset existing user settings as soon as is practicable, and in any case within [x] months of this code coming into force.

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 help you rely upon other lawful bases for processing.

For more information about lawful bases for processing, including consent, please see the supplementary guidance in Annex B.

7. 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 on 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

What do we need to do to 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 upon 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 will need to provide each element will vary.

You should avoid collecting real world identifiers whenever possible, making use of options such as avatars and user names instead.

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 needed 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 a clear signal (such as a light) so that they know their location is being tracked.

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

Example:
It is acceptable to process data about the music a child downloads if they have activated and are using a 'make similar recommendations' function of your service, but not if they are searching out content themselves without actively seeking your recommendations.

Further reading outside the code:
Guide to GDPR – data minimisation

8. 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).

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 do so. Sharing children's personal data with third parties, including sharing data inferred or derived from their personal data, can expose children to additional risks 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).

What do we need to do to 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, 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

9. Geolocation

Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, 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'?

Geo-location 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 geo-location 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.

What do we need to do to meet this standard?

Ensure geo-location options are off by default

Any geo-location tracking options should be switched off by default; with children having to actively change the default setting to allow their geo-location data to be used. The exception to this is if you can demonstrate a compelling reason for a geo-location option to be switched on by default, 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 geo-location data and prompts them to discuss this with a trusted adult if they don't understand what this 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 make the child's location visible to others is subject to a privacy setting which reverts to 'off' every 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 geo-location 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 will 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

10. 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 upon 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);"

What do we need to do to 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.

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

Age range	Guideline
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.

	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. Provide a clear and obvious sign that indicates when monitoring or tracking is active.
6-9 Core primary school years	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. 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. Provide resources to help parents explain the service to their child and discuss privacy with them. Provide a clear and obvious sign that indicates when monitoring or tracking is active
10-12 Transition years	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 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. Provide resources to help parents explain the service to their child and discuss privacy with them. Provide resources suitable for the child to use independently which explain the service and discusses privacy rights. Provide a clear and obvious sign that indicates when monitoring or tracking is active.

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

11. Profiling

Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, 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 feed 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.

Profiles are usually based upon 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 upon 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'

Profiling may also be used for purposes such as child protection, countering terrorism, or the prevention of crime.

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.

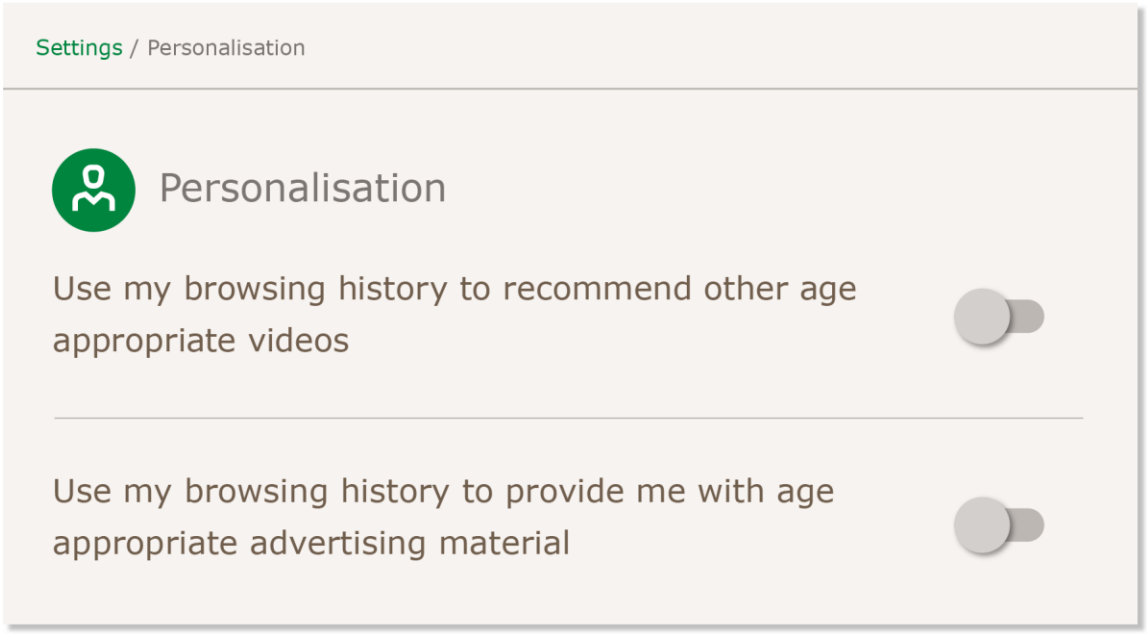
What do we need to do to meet this standard?

Differentiate between different types of profiling for different purposes

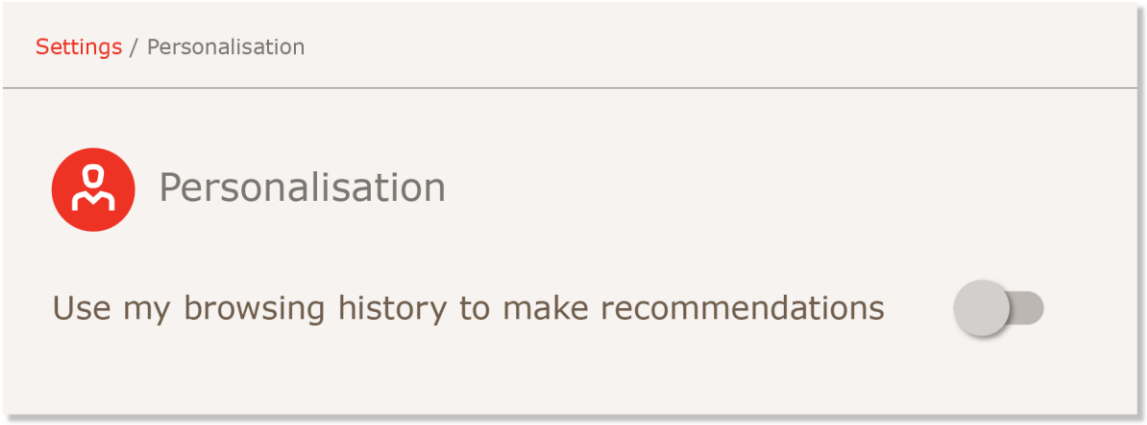
Because profiling can be used to serve a wide range of purposes it is particularly important to be clear about the purposes for which your service uses personal data to profile its users, and to differentiate between them. Catch-all purposes, such as 'providing a personalised service' are not specific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

You should offer separate privacy 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 upon 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 will need to assess this in the specific circumstances of your processing.

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

Conversely, you may have a compelling argument that you need to switch profiling for purposes such as child protection and safeguarding on by default, without the option to switch it off.

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 upon your assessment of risk and the age of the child you may wish to make further interventions, which might include age verification.

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 in order to suggest content to them then you need suitable measures in place to make sure that children aren't 'fed' or presented with 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.

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 'feeds' the content to the child. Data protection law doesn't make you responsible for third party content but it does make you responsible for what you 'feed' to children who use your service, based upon 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 will be 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 (e.g. 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 will 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.

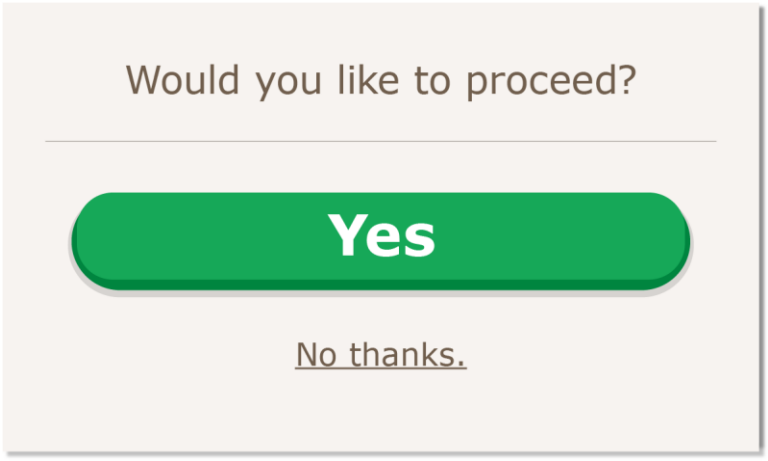
Similarly, if you cannot put suitable measures in place to safeguard children from harms arising from profiling for other purposes (such as profiling to promote certain behaviours), you should not profile children for these purposes either.

12. Nudge techniques

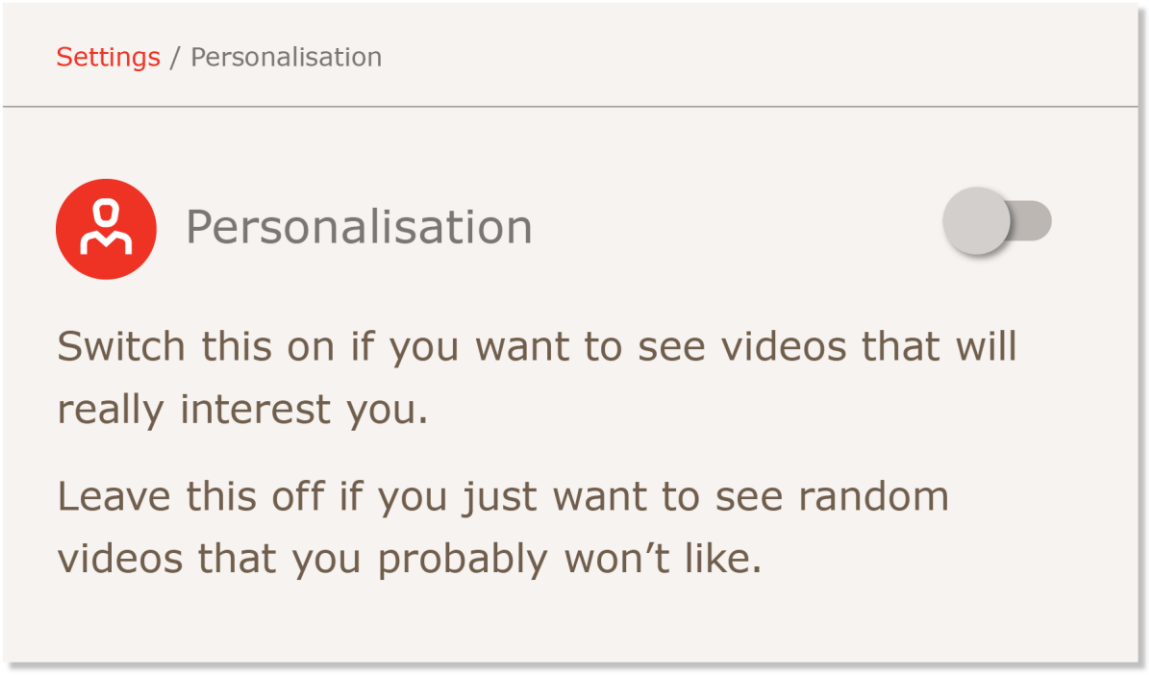
Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, turn off privacy protections, or extend use.

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 then 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.

Reward loops or positive reinforcement techniques (such as likes and streaks) can also nudge or encourage users to stay actively engaged with a service, allowing the online service to collect more personal data.

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. Or spend more time than they intend on a particular service.

Using techniques based upon 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. So does the use of reward loops or other techniques aimed at exploiting human susceptibility to reward seeking behaviours in order to keep users online. They may also run contrary to UNCRC right to be protected from economic exploitation.

What do we need to do to 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 will give you more of their personal data, or turn off privacy protections.

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

You should not use reward loops or similar techniques that seek to exploit human susceptibility to reward, or anticipatory and pleasure seeking behaviours in order to keep children engaged in your service to facilitate and maximise your collection of personal data.

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 user.

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.

At all ages you should provide tools (such as mid-level or 'anytime' pause buttons) that support wellbeing enhancing behaviours.

The table below gives some guidelines that you might wish to apply to children of different ages. Although again it is important that you carry out user testing in this area.

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

Age range	Guidelines
0-5 Pre-literate & early literacy	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. 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 upon the risks inherent in the processing. Nudge towards wellbeing enhancing behaviours (such as taking breaks).

	Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
6-9 Core primary school years	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. Provide simple explanations of functionality and inherent risk–but continue to 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 upon the risks inherent in the processing. Nudge towards wellbeing enhancing behaviours (such as taking breaks) Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
10-12 Transition years	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. Present option in ways that encourage conscious decision making. Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending upon the risks. Nudge towards wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
13 -15 Early teens	Provide design architecture which is high-privacy by default. Provide explanations of functionality and inherent risk. Present options in ways that encourage conscious decision making. Signpost towards sources of support including parents. Consider further interventions depending upon the risks. Suggest wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).

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

13. Connected toys and devices

If you provide a connected toy or device, ensure you include effective tools to enable compliance with 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 comply with 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 will 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 in place to enable you to comply with this code.

What do we need to do to 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 upon whether they are a 'processor' acting only on your behalf, or a 'controller' in their own right.

You cannot however 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. This means that both the packaging of the physical product, and your product leaflet or instruction booklet (paper or digital) should carry a clear indication (such as an icon) indicating 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 will be 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 will be 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

14. 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.

What do we need to do to meet this standard?

If order to 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 in a prominent place on the screen display.

If your online service includes a physical product, for example a connected toy or speaker you should 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 provide some guidelines.

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

Age range	Guidelines
0-5 Pre-literate & early literacy	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'. 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. Provide online tools suitable for use by parents.
6-9 Core primary school years	Provide icon(s), audio prompts or similar that children will recognise as meaning 'I'm not happy' or 'I need help'. 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. Provide online tools that children could use either by themselves or with the help of an adult.
10-12 Transition years	Provide icon(s), audio prompts or similar that children will recognise as meaning 'I'm not happy' or 'I need help'.

	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. Provide online tools that children could use either by themselves or with the help of an adult.
13 -15 Early teens	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'. 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. Provide online tools suitable for use by the child without the help of an adult.
16-17 Approaching adulthood	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'. 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. Provide online tools suitable for use by the child without the help of an adult.

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 should 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

15. Data protection impact assessments

Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. 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.

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
- 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
We have published 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 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, 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.

What do we need to do to 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 (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. 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 an existing online service likely to be accessed by children.

For existing online services, you should already have a DPIA – but you should review it (or conduct a new one) as soon as possible after the date this code comes into force. You should specifically focus on assessing compliance with the standards in this code and identifying any additional measures necessary to comply. We expect you to make those changes to your service to ensure compliance with this code as soon as possible, and in any event within [x months] of this code coming into force.

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 age-verification;
- 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 current issues of public concern over online risks to children;
- any relevant industry standards or codes of practice; 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

You should seek and document the views of children and parents (or their representatives), and take them into account in your design.

We will expect you 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 B);
- 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 comply with 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 service 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. You should consider the level of risk against each of the age ranges set out in Annex B.

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 upon children's ability or willingness to engage with your privacy information.

If you identify a particular risk to children (or to children at a particular age range or developmental stage), you can consider using age verification to mitigate this risk, either to prevent access to the service or to better tailor the service to the needs of different age ranges. However, if there is a high risk and you cannot use robust age verification to distinguish children from adults (or distinguish between particular age-ranges), you need to apply any additional safeguards to all users to make sure you mitigate the risk to those children.

In particular, and in line with the provisions of this code, if you identify a relevant risk to children you must consider (and document your decision on) whether you can implement:

- changes to the design of your service to avoid the risk;
- age verification to prevent a child accessing elements of your service that create a significant (medium or high) risk to children, especially for profiling or geolocation options; or
- positive nudge techniques where appropriate for younger children.

This is not an exhaustive list, and there may be other appropriate safeguards you can identify to mitigate any risks.

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

16. Governance and accountability

Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies procedures and terms of service demonstrate compliance with the provisions of this code.

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 to meet this standard?

Put an accountability programme in place

You should put an accountability programme in place to effectively address the standards in this code. It should be driven by your Data Protection Officer, if you have appointed one, and overseen by senior management at Board level.

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.

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

You should have policies in place that document how your organisation ensures adherence to this code and the requirements of the GDPR and PECR. 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 data protection officer);
- 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 will apply 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.

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 comply with this code

Be prepared to demonstrate your compliance with this code

You should be prepared to demonstrate your compliance with 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

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. We will monitor compliance with this code through a series of proactive audits, will consider complaints, and take appropriate action to enforce the code and the underlying data protection standards, in line with our Regulatory Action Policy. Adherence to the standards set out in this code will be a key measure of your compliance with data protection laws. If you do not follow this code, you will 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?

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 compliance?

One of the five key objectives in our Regulatory Action Policy is:

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

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

We will monitor compliance with 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 fining where necessary.

Our approach is to encourage compliance. Where we find issues we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected.

How does the ICO deal with complaints?

If someone raises a concern with us about your compliance with 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 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.

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 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 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.

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.

ISS	Information society service, as defined in Directive (EU) 2015/1535 (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 your 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.
UNCRC	The 1989 United Nations Convention on the Rights of the Child.

Annex A: 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 upon responses to the ICO's call for evidence on the age appropriate design code, ICO funded research currently being undertaken 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 & Northern Ireland.

Age/Stage	key considerations
0-5 pre-literate and early literacy	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. 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, though 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 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 pre-dominantly engaged in adult-guided activities, playing within 'walled' environments, or watching video streams. Children in this age range are less likely than older children to have their own device, though significant numbers do, and will often play on their parents' devices which may or may not be set up with child specific profiles. They are however a main user group of connected toys (such as talking teddies or dolls) and may also mimic parents' use of voice activated devices such as 'home hubs'. Children within this age range will be pre-literate or in the earliest stages of literacy, so text based information is of very limited use in communicating with them. 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 upon consent as your lawful basis for processing their personal data you need parental consent.
6-9 core primary school years	Children in this age range are more likely than younger children to have their own device (such as a tablet), though 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 still popular and they may engage enthusiastically with voice activated devices such as home hubs. 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. They are likely to be absorbing messages from school about online safety and the digital environment, and be 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. 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. Literacy levels can vary considerably and ability or willingness to engage with written materials cannot be assumed. 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 upon consent as your lawful basis for processing their personal data you need parental consent.
10-12 transition years	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). 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. 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. 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. 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. 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. Although children in this age range are likely to have more developed literacy skills they may still prefer media such as video content instead. 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. 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 upon consent as your lawful basis for processing their personal data you need parental consent.
13-15 early teens	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. The use of social media functions and applications is widespread though 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. 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. 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.

	Literacy skills are likely to be more developed but they may still benefit from a choice of media. 13 is the age at which children in the UK are able to provide their own consent to processing, if you relying upon 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)
16-17 approaching adulthood	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. 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 will still be developing and they may still tend towards risk taking or impulsive behaviours and be susceptible to reward based systems. 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 will expect a reasonable level of autonomy. Signposting to other sources of support in addition to parental support will be important. By virtue of Article 8(1) of the GDPR and s9 of the DPA 2018, if you are relying upon 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.

Annex B: 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?

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 will 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 section 7 of 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 comply with 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 comply with all the standards in this code.

You should remember that you will 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.

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

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. For example, if your DPIA identifies a risk to younger children and you are relying on parental consent as a mitigating measure, you need a robust approach to age verification and parental authorisation.

You should verify age and parental authority 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-verification mechanisms are reasonable (eg analytics cookies).

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 C: 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.

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-verification? 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? 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. Age-appropriate application:** **3. Transparency:** **4. Policies and community standards:** **5. Default settings:** **6. Data minimisation:** **7. Data sharing:** **8. Geolocation:**

9. Parental controls:

10: Profiling:

11: Nudge techniques:

12: Detrimental use of data:

13: Connected toys and devices:

14: Online tools:

16: Governance and accountability:

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