

The Children's code design guidance



ico.
Information Commissioner's Office

children's
code



Introduction

The Children's code is a code of practice that sets out how online services, likely to be accessed by children, should protect them in the digital world.

This design guidance shows how to apply some of the standards in practice, in order to create an open, transparent and safe place for children online.

Its resources focus on transparency, a common challenge for online services and a key standard within the Children's code. There are resources for other standards on the Children's code hub.

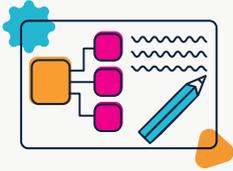
Authors:

Georgina Bourke, Ahmed Razek

Illustrations:

Big Motive (Rachel Orr)

Putting it into practice:



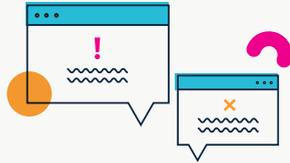
Getting started



Bring children's views into the design process



Meet children's needs as they change over time



Find the best moments to engage children with privacy information



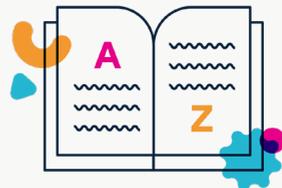
Design for meaningful parent-child conversations



Protect children's privacy by default



Practical tools for your organisation



Glossary of terms*

Glossary of terms - This will help you understand words and terms related to data protection and design within the Children's code design guidance.*

Getting started

This section outlines ways to understand and introduce the Children’s code standards into your practice.

Things to do

Check out the 15 standards of the Children’s code:

This design guidance focuses on transparency. It’s a key part of the Children’s code and touches on many design challenges in the standards.

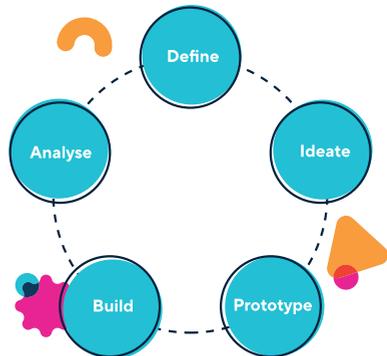
You should also familiarise yourself with the other standards in the code to understand what else your organisation needs to do to conform.

The Children’s code - the full code

ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

Embed code standards in your design process

You must consider the standards and children’s best interests at key moments in the design process to create products that conform with the code. Document important design decisions throughout to show you are meeting the standards.



Bring your teams together to plan how to conform to the code

The Children's code falls under the UK General Data Protection Regulation (GDPR). You should collaborate with people in your organisation such as your data protection officers. They already work on how your organisation complies with data protection law.

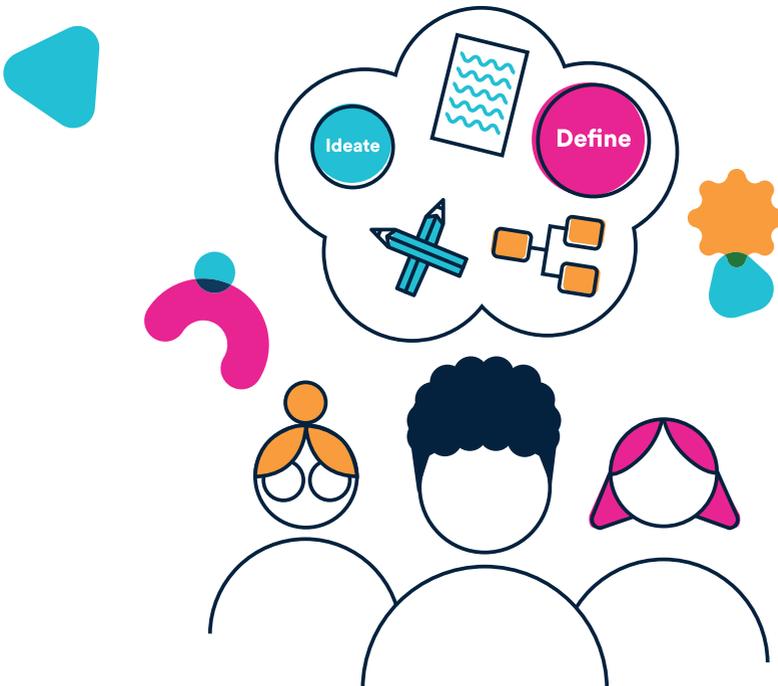
You should consider how your use of children's data either poses risks or supports their rights. You need to ensure you ultimately act in their best interests.

The ICO created a framework to help organisations:

- explore the rights children hold under the code;
- identify ways in which data use can risk or support them; and
- understand related good practice recommendations within the code.

Best interests framework

ico.org.uk/for-organisations/children-s-code-best-interests-framework



Things to avoid

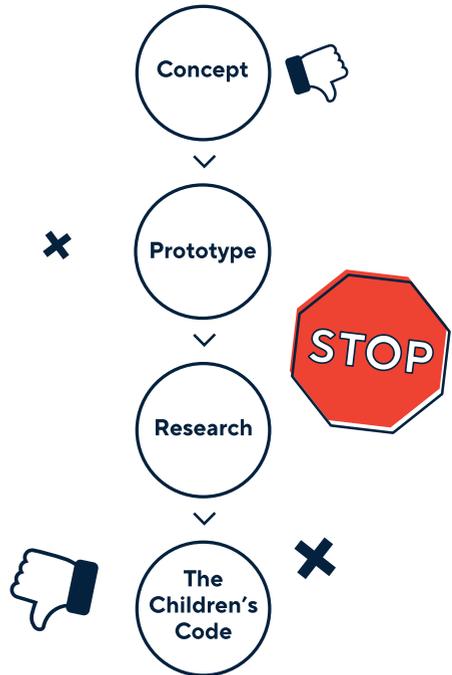
Don't think of these standards as just legal issues

Don't just rely on legal or compliance teams to meet the standards in your online service.

Designers should see these standards as creative opportunities to design engaging online experiences that put children's best interests at the heart.

Don't leave the code to the end

Think about the standards in the code at the earliest possible stage in your design process. This ensures you design products and services in children's best interests and protect their information rights.



Bring children's views into the process

This section outlines the importance of involving children in the design process so that your service meets their needs and has their best interests at heart.

Things to do

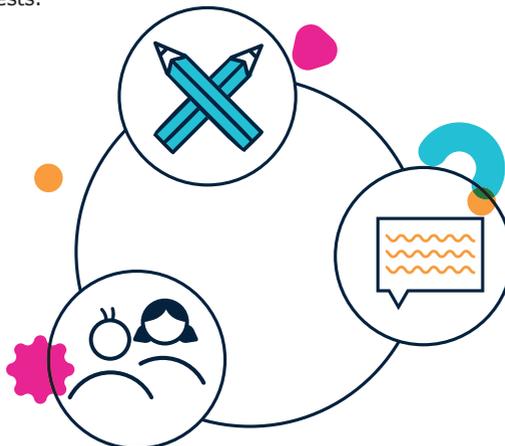
Involve children to check designs are accessible and understandable.

Choose methods that are appropriate for your specific context and scale of your product. This might include:

- Conducting user research with children to learn about their needs and test draft designs.
- Running co-creation workshops to involve children directly in design decisions.
- Collaborating with child development experts to review designs and consider children's best interests.

Use insights to support your design decisions. Work with your data protection team to include insights in data protection documents, such as data protection impact assessments.

Nielson Norman Group
Usability Testing with Minors: 16 Tips
www.nngroup.com/articles/usability-testing-minors/



Plan engagement throughout the design process

Engage with a representative sample of children at key moments in the design process:

Concept development - get early input on new ideas before they are produced.

Prototyping and research - test draft designs to check they are accessible and understandable.

Implementation - give ways to provide feedback in the service by providing '*I don't understand*' options.

Test privacy information with a representative sample of children to check it is understandable.



Things to do

Choose engagement methods that are safe and age-appropriate

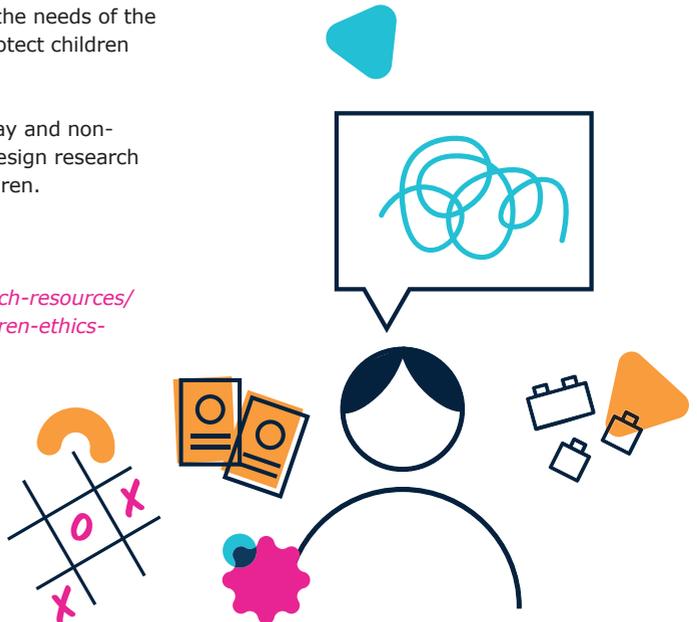
Design a research approach that prioritises children's safety and wellbeing and ensures they can contribute meaningfully.

Identify and manage any potential risks to young participants. Balance the needs of the research with the need to protect children from harm.

Explore ways to introduce play and non-verbal communication into design research approaches for younger children.

NSPCC Learning - Research with Children

learning.nspcc.org.uk/research-resources/briefings/research-with-children-ethics-safety-avoiding-harm



Things to avoid

Don't engage with children as a tick-box exercise

Ensure you engage with children with the intention of incorporating their views and needs into the design.

Design age-appropriate methods of engagement to make sure children can meaningfully contribute and feed into the design of products.





Things to check

- **Have you planned how you'll bring children's views into your design process?**
- **Have you chosen engagement methods that are safe, age-appropriate and impactful for your project?**
- **Have you ensured insights from research with children and parents influence design decisions?**
- **Have you captured research insights in your data protection impact assessment?**



Top tip!

Print off this book and mark off the check list.

Feel free to add your own notes.

Meet children's needs as they change over time

This section outlines how to design privacy information that meets children's needs as they grow and develop.

Things to do

Give younger children more support and protection

To design appropriate privacy information, you need to understand how old your users are and what their development needs might be. Children under 13 need a parent or guardian to give consent on their behalf. These age brackets are a guide for how children's needs may change as they grow:

0 - 5: Pre-literate and early literacy

Use audio or video prompts to tell children to leave things as they are or get support from a parent or guardian.

Provide full privacy information for parents.

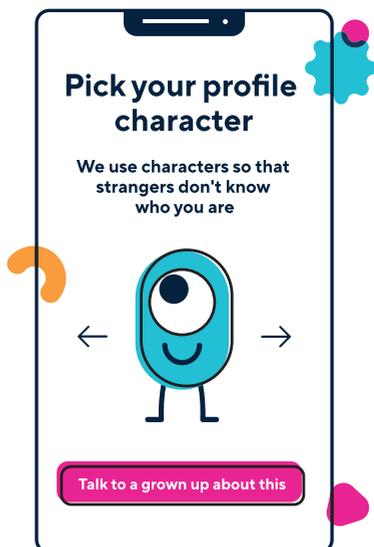
May not be able to perform advanced interactions like swipe, double tap or pinch.

6 - 9: Core primary school years

Explore using illustration, animation or sound to explain basic concepts of online privacy.

Make privacy information feel part of the user experience, rather than something separate.

Provide resources for parents to use with their children to explain privacy concepts and risks in your service.



Example of parental support:

Encourage younger children to get help with understanding privacy information.

Help older children have agency over data

Some suggestions for younger teens may also be appropriate for older teens. Interpret these in context of your service and what's right for your users.

10-12: Transition years

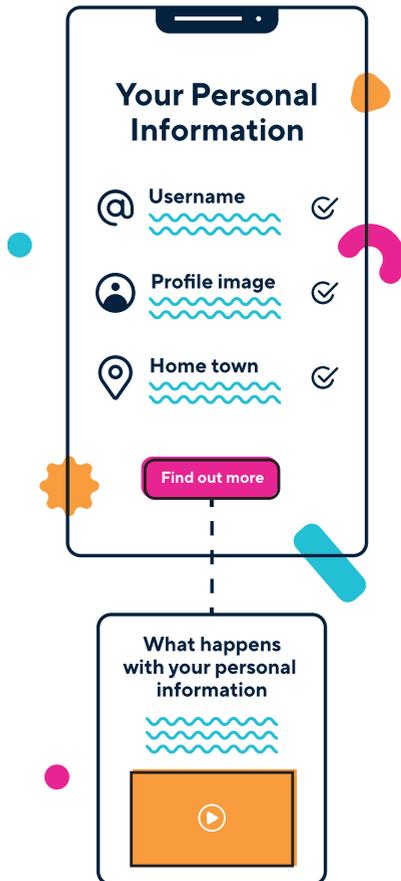
Even children who are the same age have different needs and levels of understanding. Give options for more or less detailed explanations, called 'progressive disclosure', to support different needs as children grow. Design ways for parents to support children in understanding privacy information and setting boundaries collaboratively.

13-15: Early teens

13 is the minimum age children can give consent on their own. Design opportunities for children to seek parental help as they start to make independent choices.

16-17: Approaching adulthood

Explain privacy choices clearly and neutrally so older children can understand the risks and make informed decisions about data. Prompt them to check with a parent or trusted adult if they have any concerns.



Example of progressive disclosure:

Give children the option to find out more and get more detailed explanations.



Things to do

Designing for children means designing for change

Think about how children's needs and capabilities develop as they use your product. The way you manage data-related risks, communicate privacy information and choices about data should change in response.

Different factors might signal children need a new communication approach, such as:

- using products in ways that signal developing capabilities, eg increased social interaction or sophisticated game play;

or

- external milestones that signal changes in development, eg starting secondary school or getting a personal device for the first time.

London School of Economics: Children's data and privacy online: Growing up in a digital age

www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

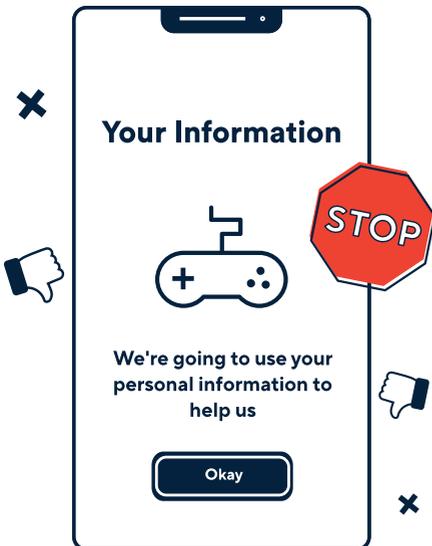
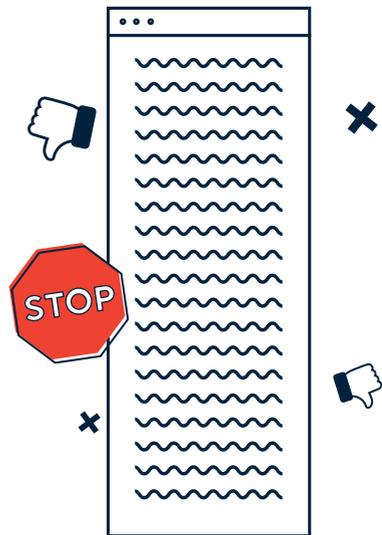


Example of external milestone privacy moment: Give children the opportunity to control what personal data they share as they develop.

Things to avoid

Don't show large amounts of text at once

Children with lower levels of literacy are likely to skip past large amounts of privacy information without reading it.



Don't simplify information to hide what is happening with personal data

Provide more detailed explanations for parents and guardians that sit alongside simpler explanations for younger children.



Things to check

- **Do you know the ages or development needs of children using your service?**
- **Have you used illustrations, audio or video to creatively communicate privacy information to children using your service?**
- **Have you designed privacy information to meet the needs of children as they grow?**
- **Have you tested your designs with children to check they find them easily and understand them?**
- **Have you identified key moments in your user journey when parents or guardians could help children understand privacy information and give consent where needed?**



Top tip!

Print off this book and mark off the check list.

Feel free to add your own notes.

Find the best moments

This section outlines how to find the right time to engage children with privacy information and understand what happens to their personal data.

Things to do

Map what data you collect and when

You should understand how you collect data in the context of your user journey to identify when and how to communicate privacy information. Look out for moments where you:

- track geolocation;
- use personalisation; or
- share data with other users or third parties.

In some cases, when children first use a product you may need to explain how your service uses data, step by step. In other situations it might be better to show privacy information in 'bite-size' chunks when you collect data. These are called just-in-time notices.



Example of a just-in-time notice:

Ask permission to access personal data when you collect it so children understand what happens to their data and why.

Find important moments in your user journey

You might need to show privacy information as the product changes:

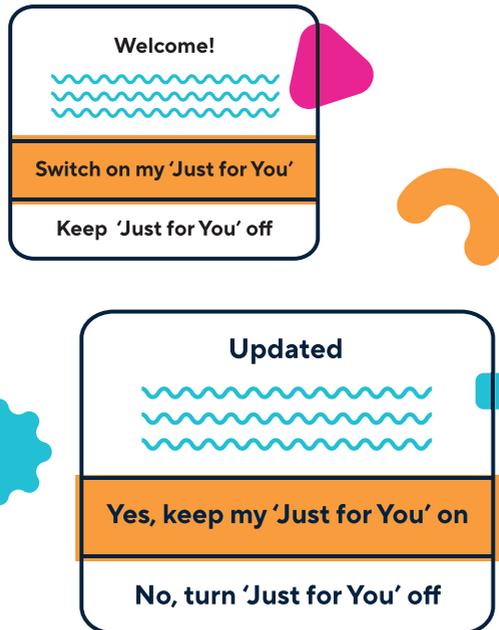
Onboarding - the first time someone understands how your product uses data.

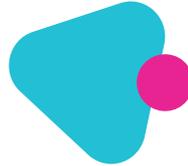
Adding or removing features - show how customising the experience affects how you use personal data.

Reviewing or changing settings - give children control of personal data on their terms.

Releasing product updates - give children the opportunity to change preferences as the product changes.

Deleting user accounts - make it easy to delete or transfer personal data at the end of the journey.





Things to do

Think about how children using the product might change privacy moments

Children using a product for the first time may not know enough about the service to make confident decisions about sharing data.

Think about other moments in your user journey where children have more time to understand what's happening to data or review their past choices.

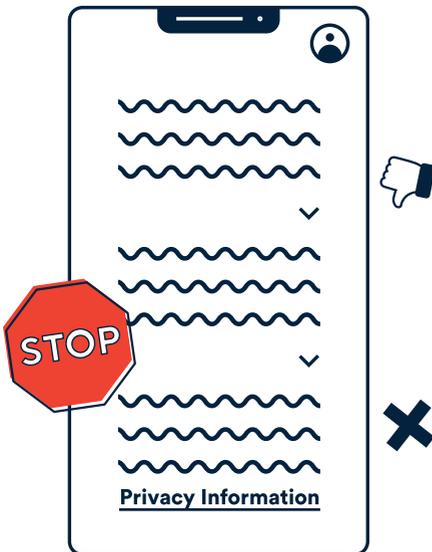
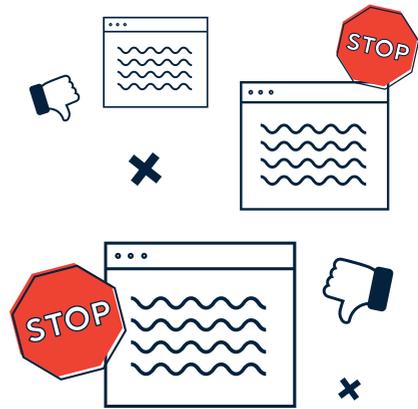


Example of reviewing a privacy decision: Give children options to change privacy decisions as they learn more about how the service work.

Things to avoid

Don't squeeze multiple privacy decisions together

Designing multiple 'just-in-time' notices in a short space of time may cause decision fatigue. Having multiple decisions to make may be overwhelming and prevent children from meaningfully engaging.



Don't hide privacy information where children won't find it

Make sure privacy information is easy to find. Don't bury important information in sub-menus that require children to click through multiple options to access it. Instead, place privacy information where children are likely to visit.



Things to check

- **Have you mapped how and when your service collects data in context of your user journey?**
- **Have you understood how key moments in your user journey might affect when and how you communicate privacy information?**
- **Have you identified how privacy moments might change as children use your service more and better understand how and why you use data?**



Top tip!

Print off this book and mark off the check list.

Feel free to add your own notes.

Design for meaningful parent or guardian-child interactions

This section outlines how to design interactions for parents and guardians to help children navigate the digital world and make informed choices.

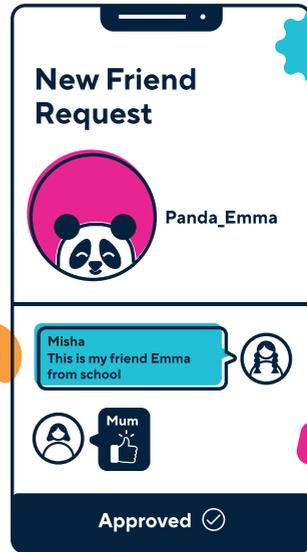
Things to do

Parental support should change as children grow

As children develop, their autonomy, independence and privacy expectations increase. Think about how the role of parental support might change over time.

There may be moments in your user journey when children are likely to need more parental support. For example, understanding how your service uses data when children first sign up or try to change a privacy setting for the first time.

Consider how to design transition moments for older children to learn to make decisions independently.



Example of collaborative decision making:
Let guardians suggest privacy settings as children start to make independent choices.

Think about parents and children's needs

Children may need to seek help from parents or guardians to understand privacy information or give consent. You need to think about parental needs as well as children's in the user experience:

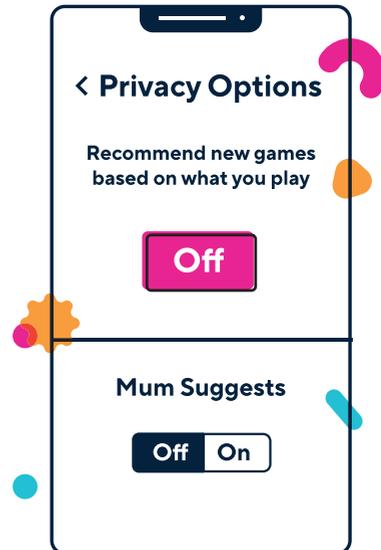
- Design privacy information that's easy for parents to find, understand and get support if they are unsure.
- Create resources to help parents discuss privacy and data with children.
- Give parents support to give consent on children's behalf or help children make decisions.

Create space for children and guardians to discuss privacy

Think about how children and parents or guardians could collaboratively make decisions about privacy and data.

Explore how families could set boundaries together rather than discreet tick-box interactions to gain parental consent.

Be transparent to children when parents are controlling or monitoring how they use products.



Example of child-guardian privacy discussion:

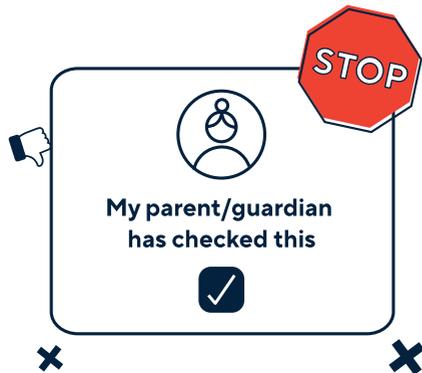
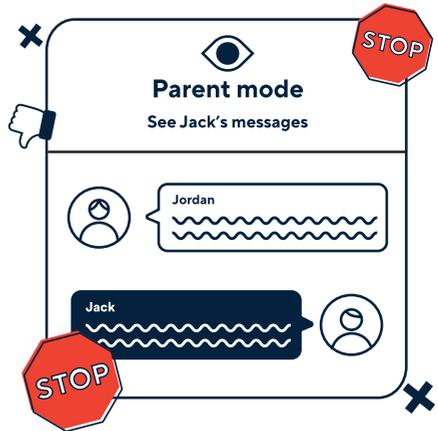
Children could talk to guardians about how they know new connections.



Things to avoid

Don't offer parental tracking without transparency for the child

If you offer parental controls, provide age-appropriate explanations and a clear signal so children know when parents are monitoring them.



Don't design parental consent controls that children can easily avoid or bypass

Design interactions that make it hard for children to avoid getting parental consent if needed. This could mean presenting a maths problem that stops children with lower literacy from going ahead without an adult. Make sure these interactions are accessible for parents.

Protect children's privacy by default

This section outlines how to design privacy settings for children so they offer the highest protection by default.

Things to do

Privacy settings must be high by default

Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking into account of the best interests of the child).

Many children just accept whatever privacy settings you provide and never change them. This is why it's important for the defaults you set to offer the highest protection.

It is not enough to allow children to activate high privacy settings. You should:

- provide them by default;
- keep them high when you update services; and
- design ways for children to revert to strong protections if they do change them.



Example of high default privacy settings:

Children's personal data is only visible or accessible to other users of the service if they change their settings to allow this.

Help children keep stronger privacy protections

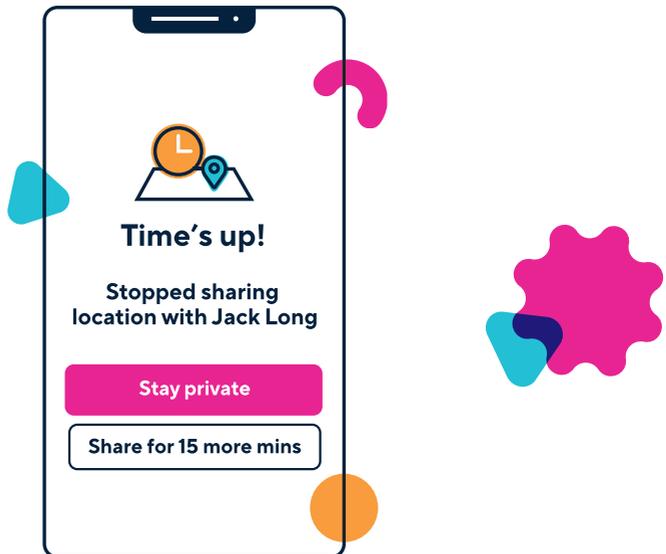
Design prompts when children try to change default privacy settings.

Younger children may need a parent or guardian to change a setting.

Older children may need clear and neutral information in context to help them make a decision. Think about ways to help children restrengthen privacy settings if they do change them.

Give them options to change privacy settings for a set amount of time, only in a specific context or when they end the current session.

Present choices neutrally or only use 'nudge techniques' (design features which lead or encourage users to follow the designer's preferred paths) to strengthen privacy settings.



Example of temporary privacy setting

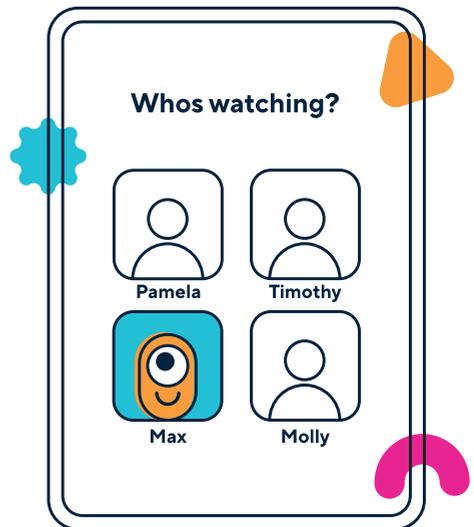
change: Share location data for a set amount of time.

Things to do

Let children set high privacy settings on shared devices

If you allow multiple users to access a service from one device, where possible, allow them to set up their own profiles with individual privacy settings. This means children don't have to share adult privacy settings when using a shared device.

Example of children's privacy settings on a shared device: Allow children to set up their own profiles and have their own privacy settings.



Things to avoid

Don't 'nudge' towards lower privacy options

Ensure your designs do not influence children to share data or follow your preferred path.

Present choices in a clear and neutral way. For younger children, it may be appropriate to 'nudge' them towards stronger privacy options.

Example of a 'nudge' that lowers privacy: Interactions that deliberately encourage children to share data.



Things to check

- **Have you set high privacy settings as default for children using your service?**
- **Have you designed prompts for when children try to change default settings?**
- **Have you thought how you can help children keep and maintain high privacy settings?**
- **Have you checked and redesigned any moments in your service where the interface design encourages children to share data, eg by using nudge techniques?**



Top tip!

Print off this book and mark off the check list.

Feel free to add your own notes.



Practical tools for your organisation

Resources to apply the code in design practice.



Create age-appropriate mindsets

Map out children's needs, behaviours and risks to help you design age-appropriate experiences.

Description

Create 'mindsets' of children who use your service to help you empathise with their needs and design services that are in their best interests.

Use these templates as a starting point. Think about children's needs and risks specific to your service and evolve the mindsets over time as you learn more from user research.

Outcomes

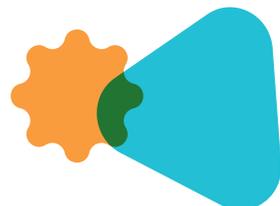
Build 'mindsets' that are based on Children's code age-appropriate design guidelines and adapted to your service

Ensure your organisation always keep children's needs in mind when designing experiences

Show how engaging with children through user research develops your understanding of their needs and behaviours

Miro Link: https://miro.com/app/board/o9J_lyNR3UI=

PDF: <https://ico.org.uk/media/for-organisations/documents/4017954/age-appropriate-mindsets-pdf.pdf>



Create data privacy moments maps

Visually map important privacy moments on to your user journey and identify risks, questions and ideas.

Description

Product teams can use this workshop to map how they use data in context of their user journey to find important privacy 'moments'.

Run the session with cross-disciplinary practitioners, such as designers, developers and data protection officers to include different perspectives.

Use the outcomes to prioritise where to improve privacy in your user experience and feed into your organisation's data protection impact assessment.

Outcomes

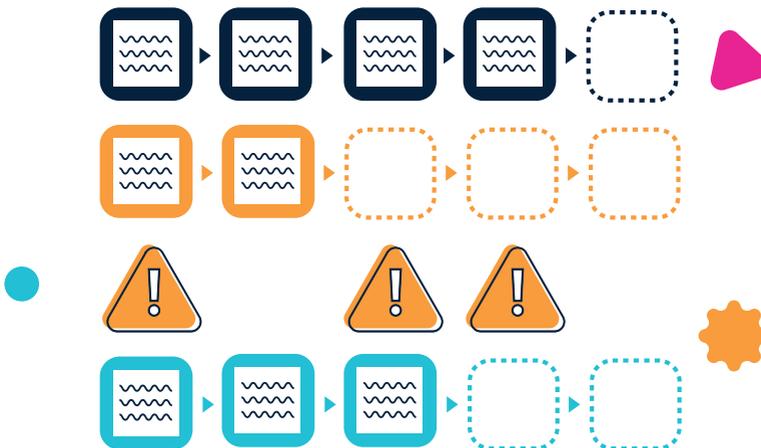
Build a shared picture of how you collect and use personal data in context of your user experience and potential impacts for children.

Collectively agree with key stakeholders in your organisation which priority areas to focus on and why.

Create a record of how you identify and address data-related risks in your user experience.

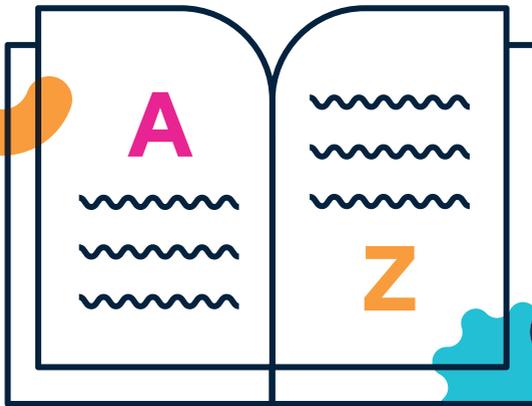
Miro Link: https://miro.com/app/board/o9J_lyMICvA=

PDF: <https://ico.org.uk/media/for-organisations/documents/4017955/data-privacy-moments-pdf.pdf>



Glossary of terms

This will help you understand words and terms related to data protection and design within the Children’s code design guidance.



Best-interests	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.”
Data privacy	The protection of personal data
Data Protection Impact Assessments (DPIAs) Personal data	A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. Organisations must do a DPIA for processing that is likely to result in a high risk to individuals.
Data protection officer (DPO)	<p>The UK GDPR introduces a duty for organisations to appoint a data protection officer (DPO) if they are a public authority or body, or if they carry out certain types of processing activities.</p> <p>DPOs assist organisations to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner’s Office (ICO).</p>
Insights	Important learnings from engagement and interaction with users.
Journey Map	A visualisation of a step-by-step process someone goes through to achieve a goal.
Mindset	Mindsets describes the way a group of people may think and what behaviours they may demonstrate as a result. Use them to empathise with different users and design to meet their needs.
Need	What the person needs from the product or service, or what problem it solves for them.
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.
Personal data	Personal data is information that relates to an identified or identifiable individual.
Risk	In this context, risk means potential harm you might expose children to because of the different ways you use their personal data.
Stakeholder	Someone who has an interest in your project, product or service.

ico.
Information Commissioner's Office



children's
code

