



Australian Government
**Office of the Australian
Information Commissioner**

Office of the Australian Information Commissioner

Extended Guide to the draft Children's Online Privacy Code



Extended guide

Contents

Introduction	3
You can ask for help to read this document.	4
Helpful Information!	6
Important fact!	6
The draft rules for the Children’s Online Privacy Code	7
Rule #1	7
Rule #2	8
Rule #3	9
Rule #4	10
Rule #5	11
Rule #6	12
Rule #7	13
Rule #8	14
Rule #9	15
Rule #10	16
Rule #11	17
Rule #12	18
Rule #13	19
Rule #14	20
Tell us what you think of the draft Code!	21

We recognise Aboriginal and Torres Strait Islander peoples as the traditional owners of the land we live on – Australia. They were the first people to live on and use the land and waters.

Introduction

The Office of the Australian Information Commissioner (OAIC) is the Australian Government's privacy regulator, and our goal is to protect the privacy of Australians.

We are responsible for writing the Children's Online Privacy Code.

When we refer to 'children' and 'young people' we mean individuals under the age of 18.

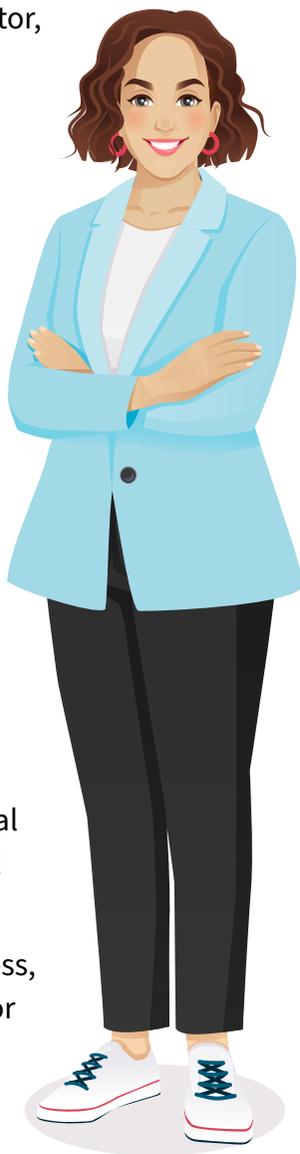
We have made this extended guide with secondary school aged children and parents and carers in mind.

But everyone is welcome to read it!

The Children's Online Privacy Code (the Code) puts children and young people at the centre of online privacy protections in Australia.

This new Code will help protect children's online privacy by telling many online services, like apps, games, and websites, how they need to follow special privacy rules when taking care of children's personal information online.

Personal information is things like your name, address, email, phone number, school, date of birth, photos or videos of you, location, and online activity.



Types of personal information



Name



Address



Email



Phone number



School



Date of birth



Photos or videos of you



Location



Online activity

Protecting your personal information online is one important step to protecting your online privacy.

Think about **online privacy** like a stage where you watch school assembly or a music concert, where the frontstage and backstage are separated by a curtain.

The frontstage is in front of the curtain and is where everyone in the audience can see what is happening. The frontstage is like where you or other people share things about you online for other people to see (like sharing photos of you with your friends and family). To help protect your online privacy frontstage, you and other people (like your family, friends, school and clubs) need to think carefully about what is shared publicly for others to see.

The backstage is behind the curtain and is where only the people running the show can see what is happening. The backstage is like where you share your personal information with an app, game, or website to use that online service. To help protect your online privacy backstage, online services need to take care of the personal information you choose to share with them.

The Code focuses on protecting your online privacy backstage. It does this by shining a light on what happens to your personal information behind the curtain, telling online services how to take care of children's personal information, and giving you more control with what happens to your personal information online.



You can ask for help to read this document.

A friend, family member or support person might be able to help you. If you speak a language other than English and need help with this document, please call the Translating and Interpreting Service on [131 450](tel:131450) and ask the operator to contact the Office of the Australian Information Commissioner on [1300 363 992](tel:1300363992).

This guide is intended to explain the main rules of the Code in an accessible way. It does not reproduce the Code's legal text, and the language has been adapted and simplified to support understanding. The official 'Exposure Draft' of the Code remains the authoritative source.

The Children's Online Privacy Code is currently a draft.

Think of it just like the first version of a speech you rehearse with your parents or carers, or a practice written response you would share with your teacher for feedback at school.

We are still planning what special rules online services should have to follow, but we are showing you what we have brainstormed so far to get your feedback.

The official draft Code is a long document filled with lots of words that relate to the law.

That is why we have worked with a group of young people to help make child-friendly guides that explain the draft Code.

The final Code must be ready by 10 December 2026.



For adults

This extended guide is intended to explain the main principles of the Code in an accessible way. It does not reproduce the Code's legal text, and the language has been adapted and simplified to support understanding by children. The official Exposure Draft of the Code remains the authoritative source.



For children and young people

This extended guide is here to help you understand the main ideas of the Code. It uses simple words instead of the exact words in the official draft. The official draft is the version that online services must follow.



Tell us what you think of the draft Code!

From **31 March to 5 June 2026** we want to hear from children, young people, parents and carers.

Have your say about the draft Code by heading to www.oaic.gov.au/privacyforkids

Helpful Information!

The Code says a lot about how online services can **collect, use, and share** your personal information. What this means is:

Online services **collect** your personal information when your personal information is handed over to them and they keep it (think of it like an online library of personal information). This might happen when you first sign up or use an app, game or website.

Online services **use** your personal information when they take the personal information they have collected from you and do things with it to help them like running the app, game or website, or to note down your interests so that it can show you ads that they know you will like.

Online services **share** your personal information when they give your personal information to another service. This might be for reasons that are to do with the actual online service, like learning how it could improve or it could be to try and get you to buy things.



Important fact!

This Code is different from the Social Media Age Restrictions, which removed under 16s from age-restricted social media platforms. You can learn more about that at www.oaic.gov.au/smma.

The Children's Online Privacy Code does not delay children from engaging in the digital world.

Rather, the Code protects children when using online services at any age, by strengthening the privacy protections of their personal information. The Code will apply to social media services, including age-restricted social media platforms where 16 and 17 year olds may have accounts.



The draft rules for the Children's Online Privacy Code

Rule #1

Many online services will need to follow the rules in the Code

This is where you can find the rules in the draft Code

Section 5-7

These online services include apps, games, and websites that are either:

- **Made for children to use,**

For example: children's versions of apps and websites, games made for children, educational apps, games, and websites etc.

- **Not made for children but children use them,**

For example: online services not specifically designed for children (i.e., they were made with adult users in mind), but children use them like messaging and social interaction apps, AI chatbots, and information service websites etc.

- **Not made for children and not used by children but a lot of personal information about children is collected, used, and/or shared,**

For example: early childhood development apps, family photo sharing apps, online school management systems that monitor student performance, and internet-connected baby monitors etc.

Importantly, the Code will not apply to all online services on the internet. But it will cover many online services that children use or concern children's personal information.

Specifically, the Code will cover online services that are either owned by organisations and companies that make over \$3 million a year, or are run by some Australian Government agencies. These specific organisations, companies and government agencies are known as 'APP entities'.

APP entities must already follow some important privacy rules called the 'Australian Privacy Principles' or 'APPs' (hence why they are called 'APP entities').

The draft Code tells APP entities that they must follow the Code's rules to help protect children's personal information online.

In essence, for children and young people this means:

Specific apps, games and websites will need to follow the rules of the new Code. Some of these will likely be common online services that you use in your daily life.

The Code will also apply to certain online services that the adults in your life (e.g., parents, carers, educators, etc.) use to record and share personal information about you and the things you do.

Rule #2

To protect children's personal information, online services might have to either give everyone better privacy protections or check the age of users

Section 8

To follow the rules in the draft Code, online services must apply these privacy protections to children's personal information.

Children are any persons under the age of 18.

If an app, game, or website is used by both children and adults, an online service might need to either:

- give everyone on its app, game, or website the same privacy protections that are required for children, or
- find out whether a person using its app, game, or website is a child or adult by checking their age.

Importantly, this age check will not stop or limit children's use of an online service.

The age check is only in place to make sure online services know which users are children so that they can make sure that the right privacy protections are in place for children's personal information.

Not every online service following the Code will need to check the age of its users.

The Code takes a 'risk-based' approach which means that online services only need to check the age of users depending on the 'risk' that there are both children and adults using the service and the particular 'privacy risks' of that service.

For example, an app that is designed for early childhood education and is used by pre-school aged children, will not need to check the age of its users because the Code will likely apply and the online service likely limits the amount of information collected.

Additionally, the way that online services check the age of users (e.g., inputting your date-of-birth, taking a selfie, uploading government ID) will also follow this 'risk-based' approach to help reduce the overcollection of information from users.

In essence, for children and young people this means:

The Code will ensure privacy protections are only applied to online services that children interact with and sometimes both children and adults use the same apps, games and websites.

If the online service does not want to check the age of people using its app, game, or website, then the Code will make the online service assume that all their users are children and the privacy protections in this Code will apply to everyone.

If the online service does not want to apply the Code to everyone, they will need to check the age of its users to make sure that the right privacy protections are in place for children.

To do this, online services might check your age by asking you to input your date-of-birth, upload a selfie, or share a government ID, to name a few ways. Importantly, checking your age will not stop or limit your access to that app, game, or website but rather protect your personal information while using that online service.

Rule #3

Online services can only collect, use, or share the bare minimum amount of personal information they need to run the app, game, or website unless you choose differently

Section 9

To follow the rules in the Code, online services must make sure that they only collect, use or share personal information that is necessary for running the service.

Think about this as the bare minimum amount of information from you required to run the app, game, or website, and nothing more.

Online services can do this having 'privacy by default' settings which means that when a child first signs up to an online service or has an account, only the personal information that is necessary to run app, game or website will be collected, used, or shared.

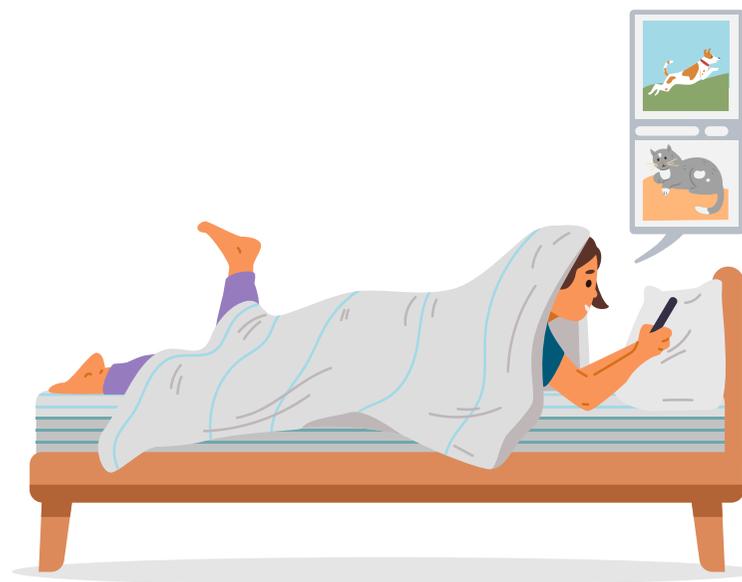
'Privacy by default' would raise the standard when it comes to privacy settings and give children and young people (or their parent or carer depending on their age) control to change their privacy settings and only allow the online service to collect, use or share more personal information than what the online service needs, if that is what they want.

In essence, for children and young people this means:

The Code will stop online services from over-collecting, over-using or over-sharing your personal information when you first sign-up or access an app, game or website.

The Code raises the standard for privacy settings by making online services only collect, use, or share the bare minimum amount of personal information from you required to run the app, game, or website, and nothing more.

The Code will make it so that if you or your parent or carer (depending on your age) are okay with the online service collecting, using or sharing more personal information than what is necessary, you can make that decision and you can change your decision back later on, if you want .



Rule #4

Online services need to be fair and take care of your personal information in a way that is best for you

Section 10–11

To follow the rules in the Code, online services must make sure that when they collect, use or share children’s personal information, it must be in the child’s best interests (meaning it is best for them and fair).

This rule in the draft Code relates to a concept called ‘the best interests of the child’.

The ‘best interests of the child’ concept comes from an international rule known as *Article 3 of the United Nations Convention on the Rights of the Child*, which states that the best interests of the child should be a primary consideration when making decisions and taking actions that affect them.

In practice this means that if an online service is collecting, using and/or sharing personal information about a child, it must consider that child’s best interests alongside their reasons for collecting the information. This includes asking things like why the collection is necessary, what the potential risks of harm associated with the collection might be, and ensuring that these reasons are consistent with the best interests of the child.

The rule in the draft Code states that if an online service’s collection, use or sharing of personal information about a child is not closely aligned with the best interests of the child, that collection, use or sharing cannot be considered **fair or lawful**.

In essence, for children and young people this means:

The Code makes online services line up their reasons for why they want to collect, use or share your personal information (and the potential risks involved in this process!) against your best interests. If it isn’t a similar match (a.k.a., if it isn’t fair), the Code says that the online service can’t collect, use or share that information from you.



Rule #5

Online services need to ask for your permission to do things with your personal information

Section 13

15-years-old or older

To follow the rules in the draft Code, if a child is 15-years-old or older, online services can now go directly to them, to ask for their permission to collect, use or share their personal information.

The age of 15-years-old and older aligns with the OAIC's current guidance on a child's capacity to consent for the handling of their personal information.

Under 15-years-old

To follow the rules in the draft Code, if a child is under 15-years-old, an online service will need to ask the parent or carer of the child (a.k.a., a person with 'parental responsibility' of the child) whom the personal information is about, to ask for their permission to collect, use or share the child's personal information.

This draft rule requires that online services must take 'reasonable steps' to confirm that permission has been given by the person with parental responsibility. Put differently, online services must make sure that the adult giving the permission is allowed to give that permission on behalf of that child.

When an online service needs permission from a person with parental responsibility, the online service must tell the child in a child-friendly (age-appropriate) way that permission has been provided by a parent

or carer, as well as information about what giving permission means for the child and their personal information (a.k.a., what the online service is going to do with that personal information).

This draft rule ensures that online services are getting permission from an individual who has the 'capacity to consent' (i.e., a person with parental responsibility), at the same time as ensuring children who are under the age of consent (15-years-old), are still involved in the process of getting permission.

In essence, for children and young people this means:

The Code makes online services recognise that if you are 15-year-olds and older, you are capable of making your own decisions about what happens to your personal information when you are online, so these services will go directly to you to get permission (known as 'consent').

If you are under 15-years-old, the Code makes online services ask your parent or carer for their permission to collect, use or share your personal information. This is because the Code recognises that under 15-years-old, you might need support when it comes to making decisions about your personal information when you are online.

Rule #6

If you are under 15-years-old, in some situations online services will need to involve both you and your parent or carer to get permission to change your privacy protections

Section 20

To follow the rules in the Code, there are specific situations where online services must ensure that the permission process involves both the child (if under the age of 15-years-old) and their parent or carer.

These specific situations are if the child chooses to allow an online service to:

- use or share their personal information for a reason beyond the bare minimum (this is known as ‘secondary use’) to run the app, game, or website (like to show targeted advertising), or
- collect sensitive information, which is personal information that needs to be treated extra carefully, like health information.

Seeking permission from a child is called ‘assent’. Assent is when a child expresses their agreement or approval to something, but that approval is not legally binding.

The draft Code explains that online services must do a **2-step permission process** in the above specific situations by first getting assent from the child, before then getting *consent* from the child’s parent or carer (i.e., the person with ‘parental responsibility’).

Consent from the parent or carer is what grants the permission because it is legally binding. If the parent or carer does not provide their consent (either ‘yes’ or ‘no’), the specific situation requested by the child cannot happen.

Importantly, when the child gives their assent to one of the above specific situations, the online service needs to explain to the child (in a way that they understand) what the consequences of their request means to their personal information and their experience of the app, game or website.

Put differently, the online service needs to explain in a child-friendly way:

- what is going to happen with their personal information, and
- that the online service will contact their parent or carer to tell them that the child has assented (agreed) to a specific change in their privacy protections and the parent or carer needs to consent (either ‘yes’ or ‘no’) for that change to happen.

This 2-step permission process recognises and puts into practice the desire held by children and young people, that they want to be more involved and aware of the circumstances surrounding why and how their personal information is collected, used, and shared online.

In essence, for children and young people this means:

The Code makes online services recognise that when you are under **15-years-old** there are specific situations that pose a higher risk to your online privacy, such as the collection of sensitive information and/or the use and sharing of your personal information for a reason beyond what is the bare minimum required.

To protect against that risk, the Code makes online services get an extra permission check from your parent or carer.

This 2-step permission process means that you get to have a say about what happens to your personal information online and work with your parent or carer as a team, to make sure that your decisions are best for you.

Rule #7

Online services must not trick you into giving them permission

Section 21

To follow the rules in the draft Code, online services must not deliberately trick, confuse, or pressure a child into giving the app, game or website permission to collect, use, or share their personal information.

This draft rule recognises that some online services may seek permission through ‘deceptive design’ practices, such as ‘nudge techniques’.

Nudge techniques are designed to influence or pressure an individual to give permission to collect, use or share more personal information than they would ordinarily agree to, if those design features were not present.

The draft Code says that if the online service does trick, confuse or pressure a child into giving permission, this permission is unlikely to be voluntary, which means the online service cannot use this permission.

Furthermore, this draft rule recognises that deceptive design practices used to collect personal information would not be considered a fair or lawful collection and does not align with the best interests of the child (remember Rule 4!).

In essence, for children and young people this means:

The Code will stop online services from tricking, confusing or pressuring you into giving them permission when they want to collect, use, or share your personal information.

This means online services must not be sneaky and hide information from you that might influence your choice when giving permission.



Rule #8

Online services must make sure that the permission they get from you (or your parent or carer) is 'good' permission

Section 14–19

To follow the rules of the draft Code, when online services ask for permission to collect, use, or share children's personal information online, they need to tick the 6 boxes below for that permission to be 'good' permission:

- ✓ without pressure, trickery or confusion so that the permission is **voluntary**.
- ✓ ensures that the child (or parent/carer) has all the right and relevant information needed to make an **informed** decision.
- ✓ asks the child (or parent/carer) often and at the right times so that the permission is **current** (because permission does not last forever).
- ✓ ensures that the child (or parent/carer) is aware that the permission can be **withdrawn** at any time.
- ✓ ensures that the child (or parent/carer) understands exactly 'why' and 'what for' the online service is asking for permission, so that the permission is **specific**.
- ✓ requires the child (or parent/carer) to take an affirmative step to demonstrate that they are giving permission for that specific collection, use or sharing of personal information, to ensure that the permission is **unambiguous** (i.e., clear).

When permission is asked for and given in the above ways, that permission is seen as 'good' permission (i.e., valid consent).

This draft rule means that if an online service does not tick the 6 boxes when they ask a child (or their parent or carer) for their permission, the permission provided cannot be accepted (i.e., invalid consent), and therefore the online service cannot collect, use or share the personal information about the child.

In essence, for children and young people this means:

The Code will make sure that online services ask for and get permission from you in a way that is fair and acceptable.

To do this, the Code sets out six rules that define what getting 'good' permission is and online services must tick off all six in order for that online service to collect, use or share your personal information.



Rule #9

Online services must make sure you can access and understand what they do with your personal information

Section 23–29

To follow the rules in the draft Code, online services that are likely to be accessed by children must make sure that their privacy policies and any notices that ‘pop up’ that tell them something about their personal information is child-friendly. That means they need to be easy to read and understood by children (no big words!).

This draft rule recognises that if an online service is made for children to use, or is not made for children but likely accessed by children, the online service should communicate in a way that speaks directly to children (i.e., child-friendly and age-appropriate language)

Examples of this include non-text-based resources like visual or audio content that can help assist children to understand the information contained in privacy policies and ‘pop up’ notices related their online privacy.

To follow the rules in the draft Code, online services must also make it easy for children (or their parents/carers) to:

- find the privacy policy documents online, in a place on the app, game or website.
- find instructions on the app, game or website that tells you how to ask for what personal information the online service knows about the child.

- ask for what personal information is known about the child and what the app, game, or website does with this information.
- request access to the personal information held by the online service. This right of access also includes the right to request information about how the online service collects, uses and shares the personal information about children.
- ‘opt out’ of receiving ‘direct marketing’ (advertising) material so to stop ‘targets ads’ being shown. For example, online services should make the ‘opt out’ button easy to find and the instructions to ‘opt out’ easy to follow.

The above draft rules ensures that online services are being transparent when dealing with children and their personal information.

In essence, for children and young people this means:

The Code will require online services to make it easy for you to find important information about how they collect, use and share your personal information.

The Code will make online services tell you about this important information in a way that you will be able to read and understand.

Understanding what personal information online services have about you and what they do with it will help you and your parent or carer (if you are under 15-years-old) make informed decisions about what happens to your person information.

Rule #10

Online services must answer you within 30 days (in most cases) if you ask to see, change or delete your personal information

Section 30–31

To follow the rules in the Code, if a child (or their parent or carer) requests to see, change or permanently delete the personal information that the online service has collected, the online service must respond within a reasonable timeframe.

To follow the rule, online services must respond to a request within a 30-day period. If it is a simple request, it should be done as soon as possible.

This draft rule recognises that there will be instances in which it will take more time to respond to the request, due to the complexity of the request and/or the online service is processing a significant number of requests, at the same time.

In some instances, the draft rule provides that the online services can extend their response time to 60 days, but if they need to do that, they need to tell the child or their parent or carer that they need more time, and they must explain the reasons why they need more time.

In essence, for children and young people this means:

The Code makes online services accountable for responding to your (or your parent or carer's) requests to see, change or permanently delete personal information records they have about you.

To be accountable, online services must respond to a request within 30 days, and if they have a good reason why they cannot respond within 30 days, they must tell you that and explain the reasons why it is going to take longer.



Rule #11

Online services must delete your personal information if you (or your parent or carer) ask for it to be permanently deleted

Section 32

To follow the rules in the draft Code, online services must say ‘yes’ if a child or their parent or carer requests their personal information records to be permanently deleted, unless there is a good reason that they cannot.

The draft rule states that examples of good reasons are if the permanent deletion would pose a serious threat to life, health or safety of an individual or the public, there is ongoing legal proceedings, or there is another law that states that the personal information cannot be permanently deleted.

The draft rule says that once the online service deletes the personal information, this is permanent and cannot be retrieved.

If a request is made, online services must action the request within a time that is fair (remember Rule 10!). If the request is a bit more complicated, online services must explain that to the child, or the parent or carer that is requesting on behalf of a child.

Online services are also required to provide confirmation that the personal information record has been destroyed. If there is a reason why they cannot action the request, the online service must provide an explanation to the child, or the parent or carer that is requesting the destruction on behalf of the child.

The provision of an explanation ensures that online services are being transparent when dealing with children and their personal information.

In essence, for children and young people this means:

The Code makes online services respect your right to change your mind about decisions you have made about your personal information online.

The Code allows you (or your parent or carer) to ask online services to permanently delete records of your personal information and online services must say ‘yes’ unless there is a good reason they can’t (like a law!).

The Code also makes online services tell you when the records have been permanently deleted. Similarly, if an online service cannot permanently delete the records, they must explain to you (or your parent or carer) why they can’t.



Rule #12

Online services must tell you when your physical location can be seen by other people and parental controls are being used

Section 33

To follow the rules in the Code, online services must tell a child if their parent or carer can:

- see or control a specific activity that the child is doing while using the online service, and/or
- see a child's physical location, through tracking the device the child is using (e.g., mobile phone, tablet, smart watch, etc.) to use the online service.

To follow the rules in the Code, online services must also tell a child if, and during the time, that any other user of the same online service can see:

- a child's physical location, through tracking the geolocation of the device the child is using (e.g., mobile phone, tablet, smart watch, etc.) to access the online service.

Online services must try their best to tell a child user about these occurrences, in a way that appropriately gets the attention of the child and is understood by the child.

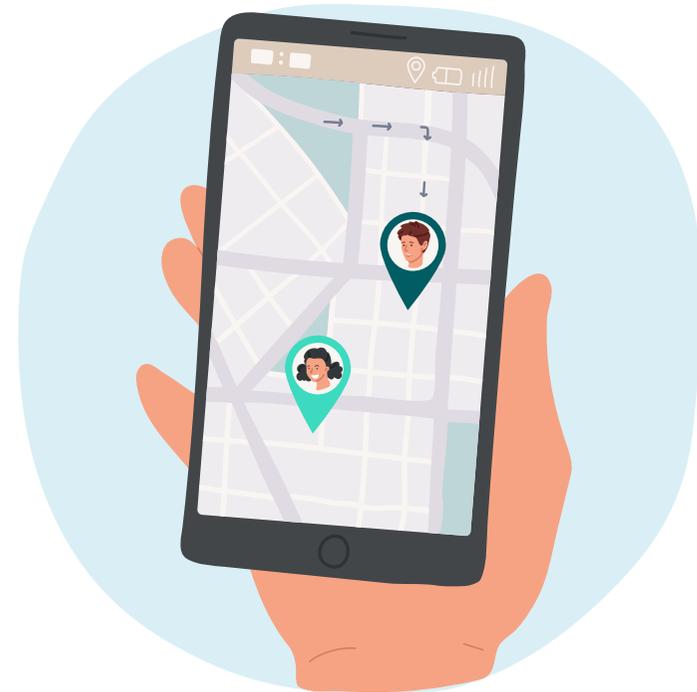
Additionally, online services must make sure that its privacy policy documents include specific information about the fact that parents and carers, and any other users, can see or control certain activities that the child is engaging with whilst using an online service (including sharing their physical location).

In essence, for children and young people this means:

The Code tells online services that they must tell you when your physical location can be seen by other people and parental controls are being used.

They must tell you when it starts happening and if possible, several times whilst it is happening. They must tell you in a way that aims to get your attention.

The Code also tells online services that they need to have this important information in their privacy policies so that you can learn more about it.



Rule #13

Online services must make it easy for you to ask questions and complain if there is a problem with your personal information

Section 35–36

To follow the rules in the draft Code, online services must give children, parents and carers, all the information they need (known as ‘privacy rights’) to ask questions or make a complaint, in a way that they can understand.

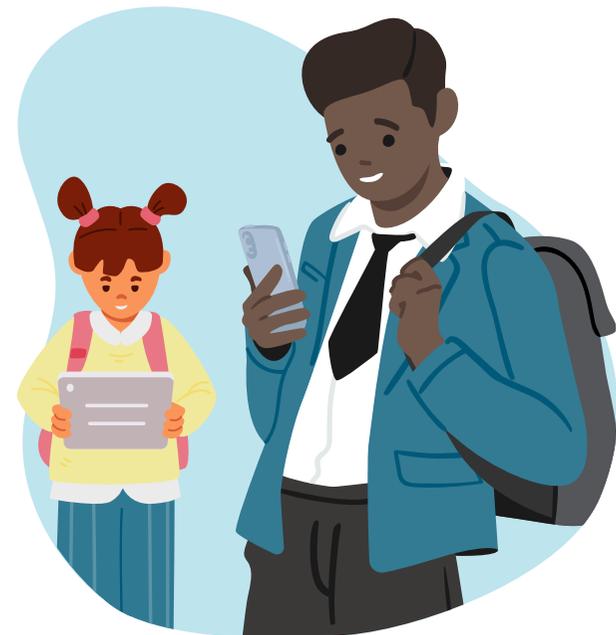
This is so that if children or their parents or carers have questions about the child’s personal information or something goes wrong in the process of the online service collecting, using, or sharing their personal information, they can easily ask a question or complain to the online service that there is a problem (this is called, ‘making a complaint’), and get assistance from the online service to resolve the problem.

Furthermore, online services must make sure that children and their parents and carers are aware that if their question is quite simple and straight forward, it can be asked anonymously.

In essence, for children and young people this means:

The Codes makes online services create an easier and friendlier path for you and your parent or carer to ask questions about your personal information or complain to the online service if there is a problem with how they have collected, used, or shared your personal information.

By making online services provide you with important information (known as your ‘privacy rights’) about how they collect, use or share your personal information, this will help you understand the types of questions you can ask online services, and what sort of problems you can complain about and what the online service might possibly say the solution could be.



Rule #14

Online services will need to think and plan before they act

Section 38–40

To follow the rules in the draft Code, if an online service wants to make a change to what they currently offer (like add a new function to the app), or the way that it collects, uses or shares personal information about a child, they must *stop, think, write and record* how they will protect children’s online privacy.

This phase of thinking and planning must be done before the proposed change takes place.

The formal name for this phase of stopping, thinking, writing and recording is known as a ‘Privacy Impact Assessment’ (‘PIA’).

To follow the rules in the draft Code, an online service must share its completed PIA with the public, by putting it on its website.

Additionally, to follow the rules in the Code, online services must make sure that any of their employees who regularly access and handle children’s personal information receive appropriate education and training to ensure that they protect children’s personal information. This education and training must be provided, at minimum, on a yearly basis.

Online services must also keep a record of this education and training to ensure that online services are kept accountable and improve record keeping of staff who have received appropriate education and training.

In essence, for children and young people this means:

The Code will make online services plan (*stop, think, write and record*) how they will protect children’s online privacy, if they are creating a new service or changing their existing service.

The Code will also make sure that the people who work for online services, who look at your personal information regularly are specialists when it comes to your online privacy.





Tell us what you think of the draft Code!

From **31 March to 5 June 2026** we want to hear from children, young people, parents and carers.

Have your say about the draft Code by heading to www.oaic.gov.au/privacyforkids



Australian Government

**Office of the Australian
Information Commissioner**

www.oaic.gov.au

copc@oaic.gov.au