

Encrypted Messaging Apps

Parent Guide

All you need to know about end-to-end encryption in messaging apps and how it can affect your children.

Age rating

*

What is end-to-end encryption?

End-to-end encryption is a communication system that **scrambles messages to stop the content from being seen or intercepted** during delivery.

This means that any encrypted message – including images and videos shared – can **only be seen by the sender and recipient**, providing more privacy and protection.

Which platforms use encryption?

The most popular platform to use end-to-end encryption is [WhatsApp](#). However, in 2021, proposed changes to its data policy led to many users opting for alternative messaging platforms.

These included **Telegram** and **Signal**.

Telegram doesn't offer end-to-end encryption by default – although it does have a **secret chat** function, with an added **self-destruct message** feature you can enable.

On Signal, all messages are automatically end-to-end encrypted. You can also equip a **disappearing messages** function, which acts similarly to the secret chat of Telegram.

What are the risks?

End-to-end encryption makes it extremely difficult for service providers to **flag the sharing of illegal content** or **high-risk conversations**.

Encryption also prevents law enforcement from **moderating** potential instances of **child sexual exploitation** – or the sharing of **abusive images**.

Grooming is also a concern, as older users may use the cover of encryption to contact younger users. These platforms do have **age restrictions**, but without a clear verification process some younger children may be able to get around this.

What should I do?

It's important that your child **understands how to stay safe** when using encrypted chat platforms – and **knows what to do** if they have a problem.

As moderators and law enforcement cannot intercept concerning messages or harmful content, they need to know **how to respond to anything that makes them feel unsafe**.

Explore the platform safety tools together – including **privacy settings** and **blocking** and **reporting** functions. Let your child know that they have **control over their messages** and who they speak to – and that they can always **leave and delete group chats** they may be in.

And let them know they can **always come to you** if anything concerns them.

**Age Rating: Whatsapp and Telegram are 16+, Signal is 12+*