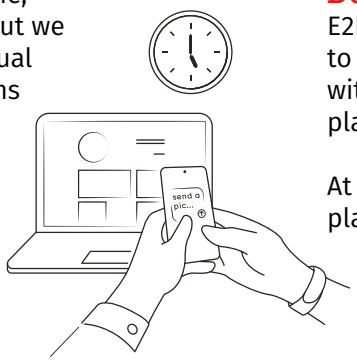
End-to-end encryption and keeping your child safe online:
A guide for parents and carers

Your child likely spends time online, and this can be full of positives, but we must also be aware that child sexual offenders may use online platforms to target children.



As many as 850,000 people in the UK could pose a sexual threat to your child, either through online or in-person abuse.[1] Recent reports from the Internet Watch Foundation (IWF) show the fastest-growing age group appearing in online child sexual abuse imagery is 7 to 10 year olds. IWF data also shows prevalence of the most severe forms of online child sexual abuse have more than doubled since 2020.[2]

Social media companies have a responsibility to keep your children safe when using their platforms by ensuring harmful messages and content, and people seeking to cause them harm are identified and reported to law enforcement.

The UK government is proposing new legislation to tackle child sexual abuse online, including removing and reporting child sexual abuse content. Companies could face enforcement action, such as a fine, if they do not comply with the rules. But parents can help too, as legislation is just one way to help keep your children safe online.

What is end-to-end encryption?

Technology companies currently use encryption positively to keep your bank transactions and online purchases safe and secure. Encryption has many other uses throughout everyday life, but some social media companies are now proposing to use, or are currently using, end-to-end encryption (E2EE) in private messaging applications and on their websites.

E2EE is a technology that messaging platforms can use which means messages are only seen by the sender and receiver. This is already present on platforms such as WhatsApp and Signal.

Recently, many social media companies have announced plans to roll out E2EE on their messaging services, including Facebook Messenger and Instagram Direct.

E2EE overrides controls that help to keep your children safe and potentially poses a huge risk.

Does E2EE pose a danger to my child?

E2EE is being introduced by social media companies to enhance privacy for their users – but if this is done without putting the necessary child safety measures in place, it could pose a risk.

At the moment, social media companies scan their platforms to find and report child sexual abuse material (such as images, videos, and grooming conversations) to law enforcement, so that abusers are arrested, and children are protected.

If E2EE is rolled out widely without necessary child safety measures, social media companies will no longer be able to find and report child sexual abuse material in the same way. It will make it harder for social media companies and law enforcement to detect child sex abusers who are looking to manipulate, groom, and sexually abuse potential victims. Crucially, it will mean that social media companies will be unable to detect and prevent the spread of images and videos of child sexual abuse within encrypted messaging services.

Currently, the information that social media companies give to UK law enforcement contributes to over 800 arrests of suspected child sexual abusers every month, resulting in nearly 1,200 children being protected from child sexual abuse.[3]

1 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file

2 https://annualreport2022.iwf.org.uk/

3 National Crime Agency data.

End-to-end encryption and keeping your child safe online:
A guide for parents and carers

What can be done by social media companies to keep their platforms safe?

It is possible for social media companies to keep their platforms safe for children, whilst also protecting privacy – it should not be a choice between the two.

Technology exists that can detect child sexual abuse material even if E2EE has been rolled out on a messaging or social media platform. Companies are making a decision not to explore or invest in these technologies. These decisions have real-life impacts for children.

Detecting child sexual abuse material is similar to detecting viruses on your computer. Antivirus software performs automatic checks on your device for viruses or harmful content to keep our personal information safe. The software will either notify you that the content is harmful or remove it for you.

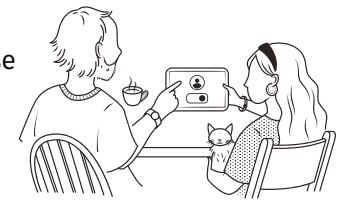
Technology exists that would work in a similar way to identify images and videos of child sexual abuse while maintaining privacy.

Social media companies have a responsibility to work with UK Government, stakeholders and charities and invest in these technologies to build a solution for their platforms that keeps children safe.

What can I do to help keep my child safe online?

Online grooming or tactics used by child sexual abusers are not always easy to spot. It is important to talk to children about these behaviours and make sure they know they have a safe place to turn if they are concerned or find themselves exposed to grooming or sexual abuse.

With the implementation of E2EE, most child sexual abuse content will go undetected. No one will be able to see those that seek to target, groom and sexually abuse children online.



Children may not know that they are being sexually abused and exploited as child sexual abusers use a range of abuse and manipulation techniques, such as posing as children online.

Whilst it is up to social media companies to ensure their online spaces are safe, there are some actions parents and carers can take to keep their children as safe as possible online.

The TALK acronym breaks these steps into four main areas. The key is to start now: whether your child has been using the internet independently for a while, or they are about to get their first mobile phone, it is not too late to take these steps.

T **Talk to your child about online sexual abuse. Start the conversation and listen to their concerns.**

A **Agree ground rules about the way you use technology as a family.**

L **Learn about the platforms and apps your child loves. Take an interest in their online life.**

K **Know how to use tools, apps and settings that can help to keep your child safe online.**

For support on having these conversations visit talk.iwf.org.uk

Additional support for you and your child

If you think a child is in immediate danger, phone 999.

If you have any concerns about a child's safety or well-being, contact the NSPCC Helpline on 0808 800 5000 or email help@nspcc.org.uk

If you are concerned about a child or young person, find out how to contact their local children's social care team at www.gov.uk/report-child-abuse-to-local-council

If you are worried about online sexual abuse or grooming of under 18-year-olds, you can report it to the National Crime Agency's CEOP Safety Centre at www.ceop.police.uk/safety-centre

For further advice there are a number of organisations that can help, visit the Internet Watch Foundation website for details: talk.iwf.org.uk/additional-help