What is a deepfake?

Guidance for parents and carers

Stay informed about AI and deepfakes to keep your child safe online.

internet matters.org

What to know

Deepfakes are fake images, videos and audio that look and feel like genuine content.

Often, they use real people to make it seem like they are doing or saying something they haven't said.

A **nude deepfake** is where an image or video has been manipulated or generated to remove or partially remove clothing from someone. People creating deepfakes use artificial intelligence (AI). AI cannot independently create deepfakes without human instruction.

Risks of deepfakes

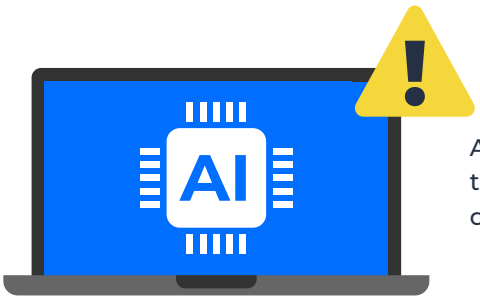
Deepfakes can impact children in the following ways:

Child sexual abuse material (CSAM): In 2023, the Internet Watch Foundation (IWF) found over 11,000 images of AI-generated CSAM on one dark web forum. Additionally, around 98% of deepfake videos are non-consensual sexual imagery.

Mis/disinformation: Many popular deepfakes feature public figures such as politicians or celebrities. In some cases, people might use deepfakes to persuade the public to believe in certain ideas or agendas.

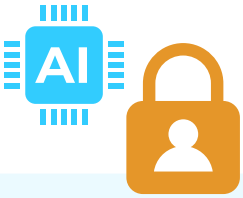
Sextortion: If a perpetrator uses deepfakes to create CSAM, they might threaten the victim in exchange for either money or real nude images. The threats usually involve releasing the images to family and friends. Research shows that children find this a scarier prospect than the sharing of real images of them.

Scams: In addition to sextortion, children (or their parents) might fall victim to other types of scams – such as voice-cloning – where the perpetrator pretends to be a family member in trouble. Often, the victim is falsely told that they must send money to help the family member.



Additionally, children and young people impacted by the above risks might feel embarrassed or humiliated, damaging their sense of wellbeing.

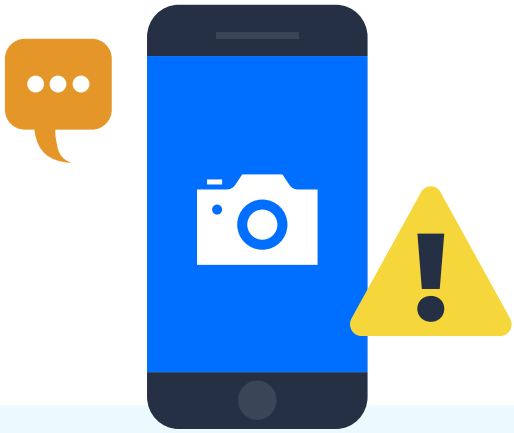
How to limit risks and prevent harm



Child-sexual abuse material

- To create deepfakes, criminals need to have real images, videos or audio to 'teach' the AI. So, avoid publicly sharing photos, videos or other recordings of your child online.
- Make sure your child knows to avoid sharing content of themselves online.
- Keep your and your child's online profiles private. If someone requests to be their 'friend', make sure they check with you first and set parental controls to limit this where possible.

If you find an image of your child online, use the Report Remove tool from Childline to get it taken down.



Sextortion

- Ensure your child feels comfortable talking to you about scary or embarrassing issues like sextortion. You can do this by regularly and openly talking about their online lives and how to get help.
- Talk about the signs of inappropriate behaviour that could lead to sextortion such as requests to do things that make them uncomfortable.
- Assure your child that you are here to help them and that it's better to feel embarrassed and tell you what's happening than to keep it to themselves.

In addition to regular conversations about who they talk to or interact with, set parental controls across apps and platforms to limit who can contact your child.

Mis/disinformation

- Encourage children to question everything they see online, especially where a public figure is saying something controversial or someone from school is featured in strange content. If they're unsure, they can ask you or another trusted adult.
- Practise fact-checking content together. You can do this by finding images or videos on social media or through other sources (whether they are AI-generated or not).
- Show your child how to use fact-check resources like Snopes and Full Fact.
- Use reverse image-searching tools such as Google Lens. To do this:
  - Go to Google.co.uk. In the search bar, click the camera icon to the right of the microphone.
  - Upload the image or enter the image URL (must end in a file name such as .PNG or .JPG).
  - Click 'Find image source' above the uploaded image.
  - If you click through to the page it sits on, you can learn more information, which can help you learn if it's AI-generated, another form of misinformation or a truthful image.

Remember that fact-checking is a key media literacy skill and requires critical thinking. Children will need to practise this skill with you to improve their ability.

Scams

- Create a secret code with your child. If you/they ever receive a panicked call, ask for the code to check that it is the actual person calling. It should be something memorable and private to you both.
- Give your child tools to quickly check if something is legitimate:
  - Encourage them to ask a person on their regular email/number if someone is saying they're in trouble.
  - If receiving an email, check the email address (not just the name) to see if it's the sender's normal email.
  - Avoid clicking on any links or opening any attachments if you are suspicious about the sender. Ignore, report and delete such messages.

Remember to help your child report scams to Action Fraud (or the police by dialling 101 in Scotland). You can also forward phishing emails to report@phishing.gov.uk and text messages to 7726.

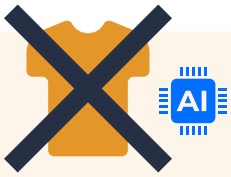
Resources to prevent deepfake harm

You can help protect children and young people from harm due to deepfakes by staying informed.

Explore the resources below to learn about a range of issues related to deepfakes. Find expert guidance and tips to help your child stay safe online.

What is a deepfake?

Get more information about deepfakes to help manage the risk children face online.



What is undress AI?

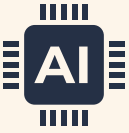
Learn about nudifying apps, the risks, the law and how to protect children.

What is sextortion?

Find information on 'sextortion' of children along with guidance on prevention.

Online critical thinking guide

Get tips for developing children's key critical thinking skills for online spaces.



Making the most of AI

Learn about the positive opportunities that generative AI tools can offer families.

My Family's Digital Toolkit

Get personalised online safety advice that keeps up with your child's digital needs.

Scan below or visit **internetmatters.org** for more advice

InternetMatters
@im_org
@InternetMatters
Internet Matters Ltd
@internetmattersorg
@InternetMatters_org

internet matters.org