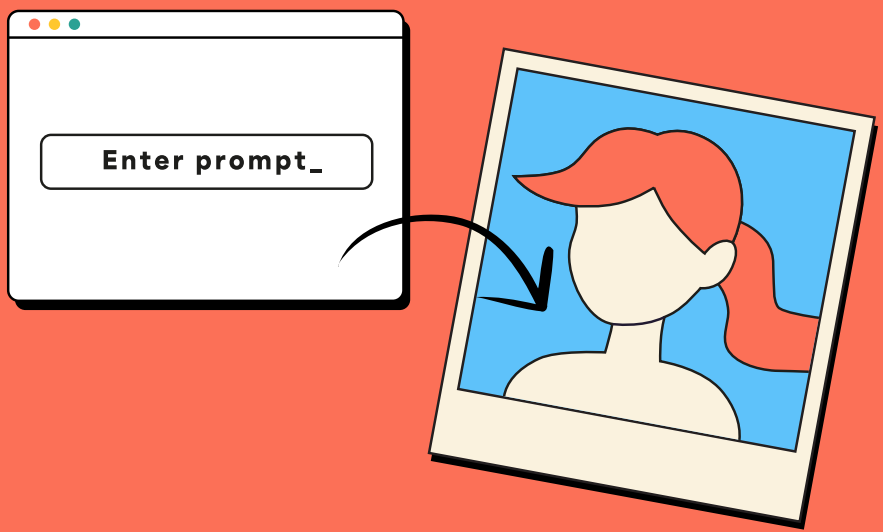
JUNE 2026 | ENGLAND

Child sexual abuse material generated by artificial intelligence

An essential guide for professionals who work with children and young people



NCA National Crime Agency

CEOP Education from the National Crime Agency

IWF Internet Watch Foundation

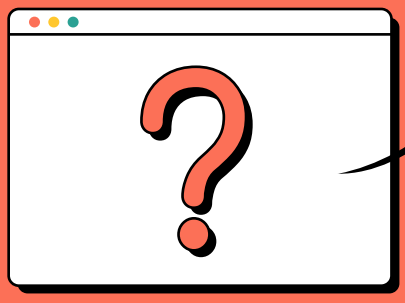
Working together to stop child sexual abuse online

Why you need to know

Developments in artificial intelligence (AI) come with a range of benefits, including supporting learning, creativity and innovation.

There is however growing concern for how AI can also be misused to create and share child sexual abuse material (CSAM), referred to as AI-CSAM. **Under UK law, AI-CSAM is illegal.**

In their **2025 Annual Data & Insights Report**, IWF recorded 8,111 AI-generated child sexual abuse images and videos from 498 reports - an increase of 154% on 2024's reports.



As professionals working with children and young people, understanding these risks is essential to help protect them from potential harm and to respond effectively to incidents.

AI describes computer systems that mimic human intelligence to solve problems, make decisions and automate tasks. **Generative AI** is a type of AI that can create new content, such as text, images, videos and audio.

Examples of AI models include:

- **Text-based models (Large Language Models - LLMs)** such as ChatGPT, Microsoft Copilot, Google Gemini and Meta AI.

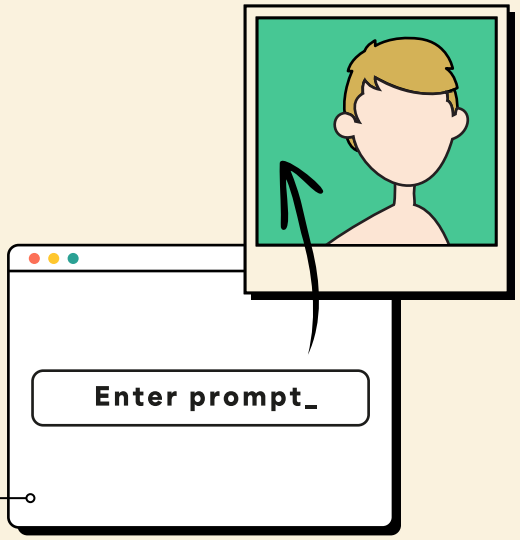
- **Image generation models,** where AI images are created by inputting descriptive language or other images such as Midjourney, DALL-E and Adobe Firefly.

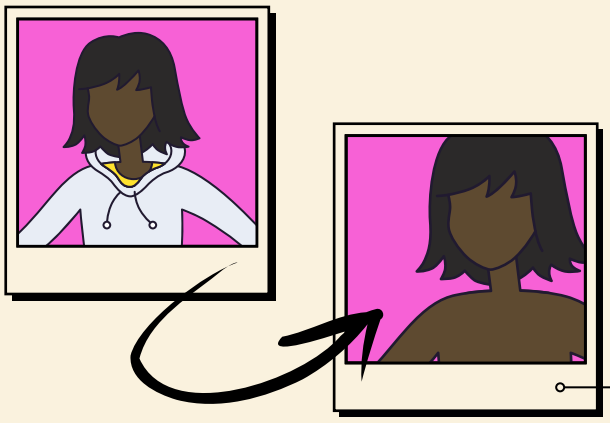
How is AI used to create CSAM?

Some of the ways AI can be used to create CSAM include:

AI can be used to create highly realistic (often referred to as **photorealistic**), manipulated images and videos of a child or young person.

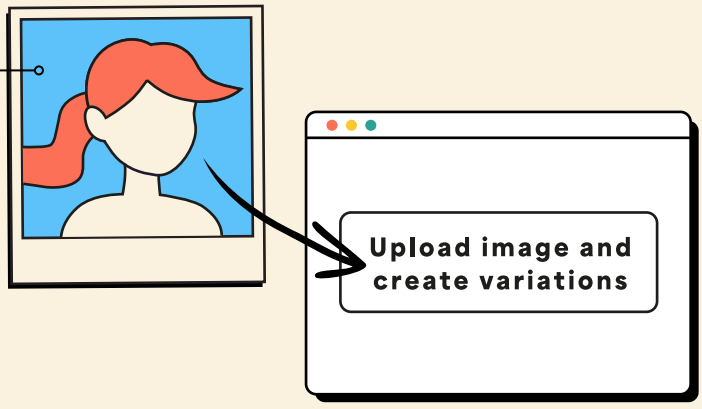
This can be done by **altering existing photos or videos or creating entirely AI-generated sexual abuse content.**



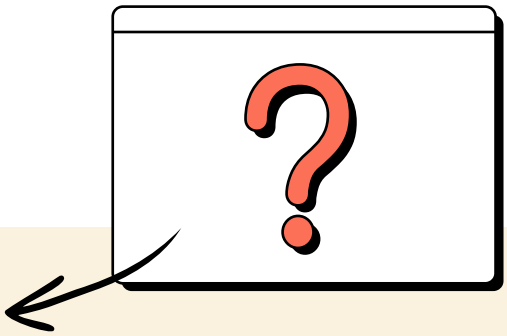


'Nudifying' or 'undress' AI tools can be used to digitally remove clothing from images creating sexual abuse imagery of a child or young person.

Utilising real child sexual imagery to feed AI models to **create new image sets and videos** of existing survivors.



Your questions answered



How do I know if an image or video is AI-generated?

It is not your responsibility to work out how CSAM has been created, or whether any part of it is AI-generated. Any child sexual abuse material online should be reported immediately to police and your setting's Designated Safeguarding Lead (DSL) or equivalent.

What if AI-CSAM is not photorealistic?

It is still illegal, even if the material is not photorealistic. It is an offence to possess a prohibited image of a child, including AI-generated images which are not deemed photorealistic, including cartoons, illustrations and animations. (Section 62 of the Coroners and Justice Act 2009).

What if a young person in my setting is making AI-CSAM of their peers?

There have been cases where young people have used AI to create nude images of their peers. This should be treated the same way as any other CSAM safeguarding concern.

Report it immediately to your setting's Designated Safeguarding Lead (DSL) or equivalent. Follow your setting's child protection and safeguarding procedures.

Is AI-CSAM illegal in the UK?

Yes, child sexual abuse material is always illegal, regardless of how it is created.

Section 1 of the Protection of Children Act 1978 criminalises the taking, distribution and possession of an "indecent photograph or pseudo photograph of a child" (anyone under the age of 18).

The use of AI does not lessen the impact or harm caused to victims. The harm to victims is always significant, regardless of the method used to create the CSAM.

Why would someone create AI-CSAM?

Offenders may use AI to create CSAM for a range of reasons, including a belief that what they're doing is less harmful as they're not in direct contact with a child; a belief that they're less likely to be caught; or that AI-CSAM is 'victimless'.

They may also create AI-CSAM as a way to blackmail a child into sending them indecent images, or for financial gain where they threaten to release the images of the child unless payment is made (Financially Motivated Sexual Extortion).

Where an under 18 is creating AI-CSAM, they may think it is 'just a joke' or 'banter' or do so with the intention of blackmailing or harming another child. They may or may not recognise the illegality or the serious, lasting impact their actions can have on the victim.

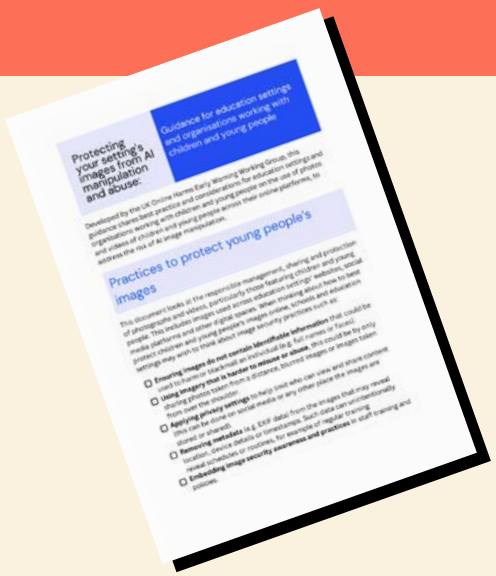
Consent forms

Settings that work with children and young people should regularly review their image consent processes to ensure they remain appropriate and are understood by families, considering whether images featuring children and young people are required at all.

Image consent forms should clearly set out how photos and videos may be taken, stored, shared or published, including online use and the potential for wider sharing. They should also make it clear that consent can be limited or withdrawn at any time.

As there are risks associated with AI enabled image misuse, **it is good practice to:**

- inform parents and carers how AI can be misused to create CSAM using everyday images, ensuring they are able to give informed consent
- revisit consent forms with parents and carers at key transition points, such as the start of a new academic year
- involve children and young people in discussions about consent, privacy and how their images are used
- continue to communicate with parents and carers about image consent to reduce safeguarding risks and reinforce shared understanding around the use of imagery by your setting


Protecting your setting's images from AI manipulation and abuse

Guidance for education settings and organisations working with children and young people

Practices to protect young people's images

Protecting your setting's images from AI manipulation and abuse

Guidance has been developed by the **UK Online Harms Early Warning Working Group on best practice and considerations for education settings and organisations working with children and young people** on the use of photos and videos across their online platforms, to address the risk of AI image manipulation.

The guidance looks at the responsible management, sharing and protection of photographs and videos, particularly those featuring children and young people. This includes images used across education settings' websites, social media platforms and other digital spaces.

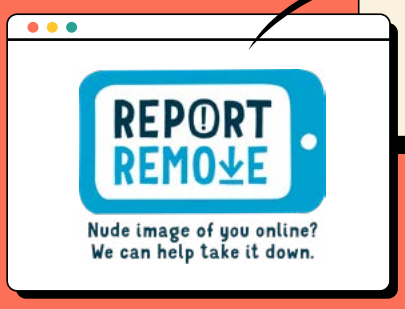
You can read the guidance and complete the actions checklist from the **UK Safer Internet Centre** to protect young people's images.

Responding to an incident

Any incident involving AI-CSAM should be treated with the same level of care, urgency and safeguarding response as any other incidence involving child sexual abuse material.

1. **Report it** to your DSL or equivalent.
2. **Follow the child protection and safeguarding policies** and procedures in your setting.
3. **Do not share, download or save the content** - even for reporting purposes. The decision to view any imagery should be based on the professional judgement of the DSL (or equivalent). The DSL should never copy, print, share, store or save them; this is illegal. For further information, please see UK Government's Guidance **'Sharing nudes and semi-nudes: How to respond to an incident'**
4. **Encourage the young person not to delete anything** that could be used as evidence, such as messages, images, videos, usernames and URL links.
5. **Report it to the site, app or network** hosting it.
6. **Report it to the Police.** Call 101, or 999 if you believe the child or young person is in immediate danger.
7. **Consider wellbeing support.** As with any form of CSA, victims may need support to manage the emotional and psychological impact. Make victims of AI-CSAM aware of support in your setting and locally.

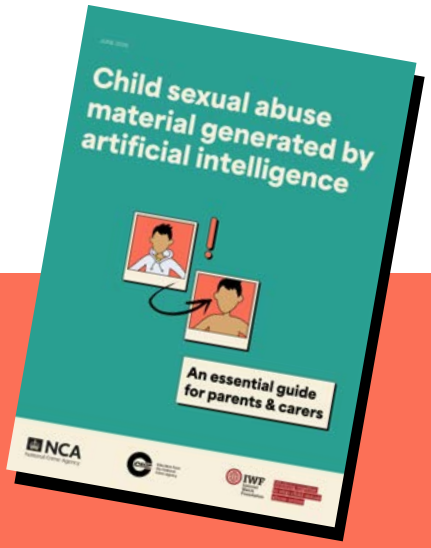
For further guidance on responding to incidents and reporting to statutory services, (including the police) visit: **sharing nudes and semi-nudes: advice for education settings working with children and young people.**



Children and young people can use the Report Remove tool from the IWF and Childline to report AI-CSAM that has been shared or might be shared online.

If a child or young person is in immediate danger report to the police by calling 999.

Guidance for parents and carers



We have created a dedicated resource for parents and carers to support their understanding of the misuse of AI and how to support their child if an incident occurs.

The guidance helps parents and carers to:

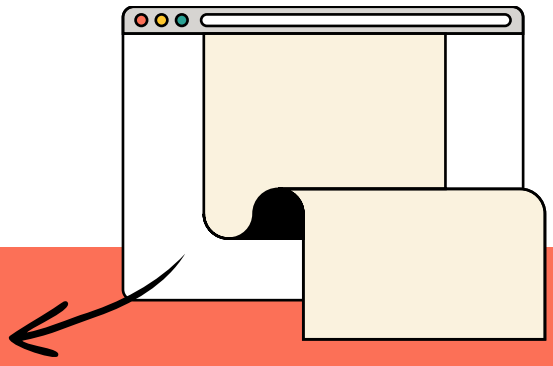
- Understand what AI is and how it can be misused to manipulate or generate CSAM
- Recognise that CSAM can include nude or semi-nude images, cartoons or AI generated content, and is illegal under UK law
- Take practical steps to reduce the risk of AI image misuse, including reviewing privacy settings, auditing social media accounts and revisiting image-sharing consent forms
- Have open, age-appropriate conversations with their child about AI and its misuses, and image consent.

How you can use this guidance

Professionals working with children and young people can use this guidance to:

- Reinforce safeguarding messages at home
- Support ongoing conversations with parents and carers about image sharing and consent
- Signpost families to appropriate reporting routes and support services if an incident occurs

Further info



- UK Council for Internet Safety guidance, **sharing nudes and semi-nudes: advice for education settings working with children and young people**
- IWF report **How AI is being abused to create child sexual abuse imagery**
- NSPCC's **guide to managing incidents of problematic or harmful sexual behaviour**
- **Generative AI YouTube playlist** for professionals from London Grid for Learning (LGfL) - includes the harms landscape and what schools need to know/do
- NSPCC's **Viewing Generative AI and children's safety in the round**
- The **Marie Collins Foundation** has produced a written **summary of legislation** in England and Wales for offences relating to indecent images of children
- Centre of expertise on child sexual abuse (CSA Centre) **communicating with children guide**, giving professionals the knowledge and confidence to speak to children about sexual abuse

Glossary

Dark Web: a secret network and a series of websites hidden from the public, and inaccessible through traditional search engines like Google.

Photorealistic: The creation of images that are so realistic, they are indistinguishable from photographs.

Large Language Models (LLMs): A type of AI programme that can recognise and generate human language text. They work by analysing large data sets of language.

Nudify: The digital process of altering existing images or videos to remove clothing from someone, making them appear as being nude or semi-nude. When used to create images of anyone under 18, this is classed as child sexual abuse material and is illegal.

Deepfake: AI-generated or AI-manipulated images, videos or audio content that falsely represents a person as saying or doing something they did not do, often designed to appear realistic and/or authentic. large data sets of language.

CEOP Education from the National Crime Agency

The CEOP Education programme offers a range of free resources for professionals, parents/carers and under 18-year-olds on the threat of online child sexual abuse, visit ceopeducation.co.uk to find out more.