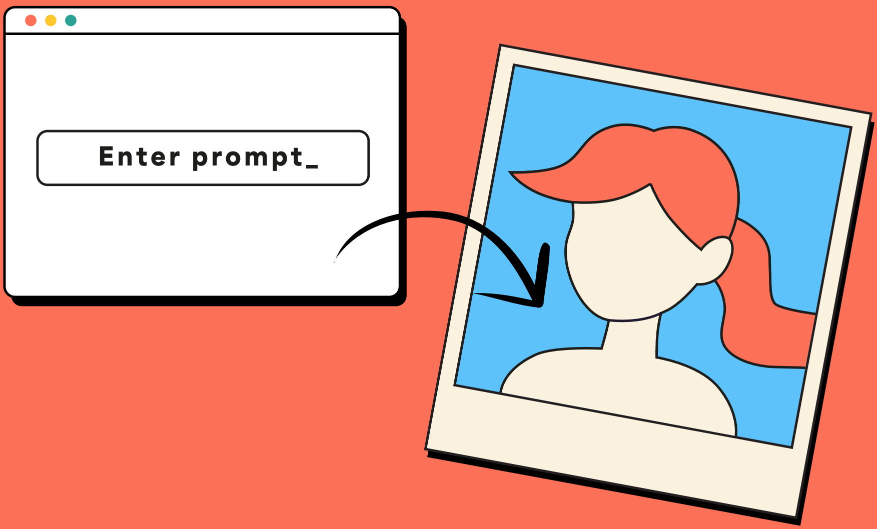
JUNE 2025 | SCOTLAND

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

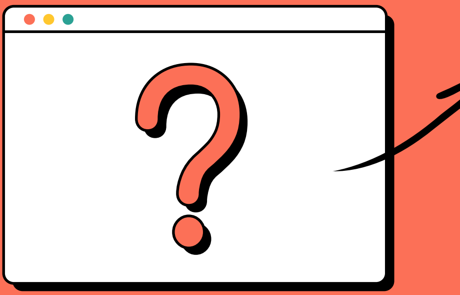
Education Scotland
Foghlam Alba

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 **2024 report,** IWF observed a rapid increase in the number of AI CSAM reports, both on the clear web and **dark web** forums.



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.

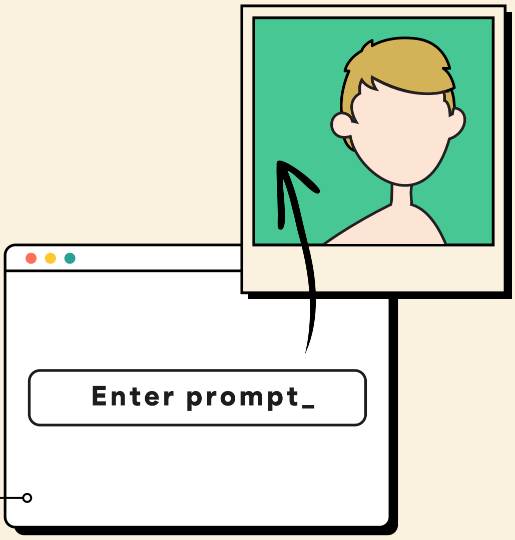
- **Image generation models,** where AI images are created by inputting descriptive language or other images such as Midjourney, DALL-E and Adobe Firefly.

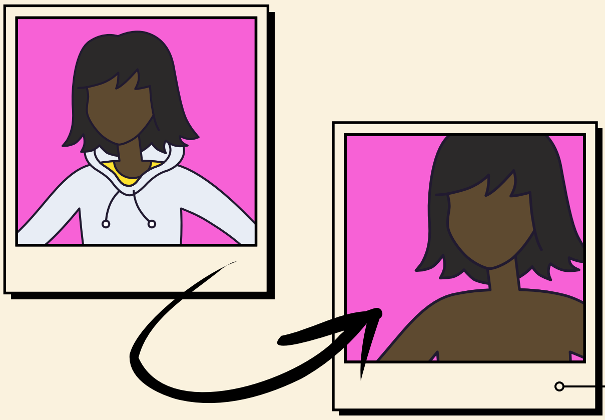
How is AI used to create CSAM?

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.

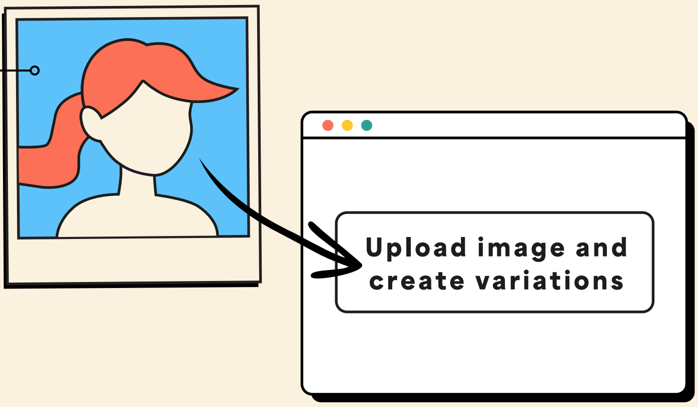
This can be done by **altering existing photos or videos or creating entirely AI-generated sexual abuse content.**



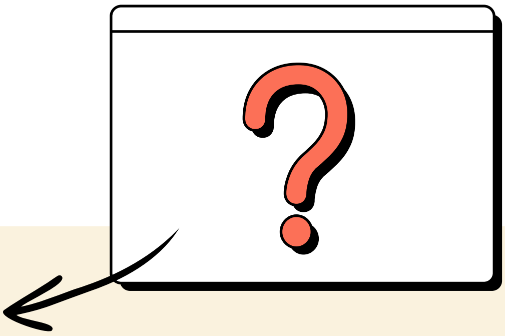


'Nudifying' or 'undress' AI tools can be used to digitally remove clothing from images creating sexual abuse imagery of a child or young person.

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 Child Protection Officer (CPO) or equivalent.

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 Child Protection Officer (CPO) or equivalent. Follow your setting's safeguarding and child protection procedures.

Is AI-CSAM illegal?

Yes, child sexual abuse material is always illegal, regardless of how it is created. Section 52 Civic Government (Scotland) Act 1982 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).

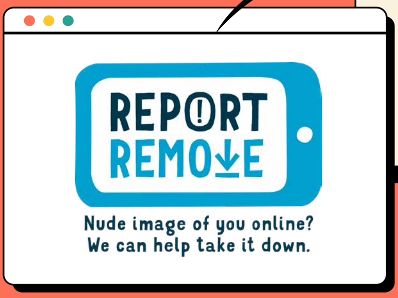
Where an under 18 is creating AI-CSAM, they may think it is 'just a joke' or 'banter' or do so with the intention of blackmailing or harming another child. They may or may not recognise the illegality or the serious, lasting impact their actions can have on the victim.

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 CPO** or equivalent.
2. **Do not share, download or save the content** - even for reporting purposes. Do not view any imagery unless absolutely necessary. The decision to view any imagery should be based on the professional judgement of the CPO (or equivalent). The CPO should never copy, print, share, store or save them; this is illegal.
3. **Follow the child protection and safeguarding policies** and procedures in your setting.
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 Police Scotland.** Call 101, or 999 if you believe the child or young person is in immediate danger.
6. **Report it to the site, app or network** hosting it.
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.

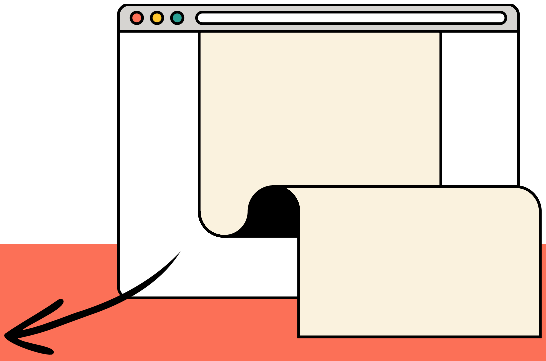
Children and young people can use the Report Remove tool from the IWF and Childline to report AI-CSAM that has been shared or might be shared online.



Nude image of you online?
We can help take it down.

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

Further info



- IWF report **How AI is being abused to create child sexual abuse imagery**
- Police Scotland's information on **Online child sexual abuse**
- Education Scotland's resource pages:
    - **Child Sexual Abuse (CSA)**
    - **Online abuse and exploitation**
    - **Identifying, understanding and responding to sexual behaviours in young people**
- NSPCC's **Viewing Generative AI and children's safety in the round**
- **Generative AI YouTube playlist** for professionals from London Grid for Learning (LGfL) - includes the harms landscape and what schools need to know/do

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

Generative AI: The use of AI to create new content including text, images, audio, videos, and other content using existing data.

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.

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.