Parents and carers

AI-assisted image-based abuse: Navigating the deepfake threat

What is image-based abuse involving AI deepfakes?

'Deepfakes' are extremely realistic images, videos and audio that show a real person doing or saying something that they did not actually do or say.

Nude or sexual deepfakes created using artificial intelligence (AI) are images, videos or audio that depict real people in sexually suggestive or explicit situations that did not take place.

Image-based abuse is when someone shares, or threatens to share, an intimate image or video of a person without their consent. This includes nude or sexual deepfake images or videos created by AI.

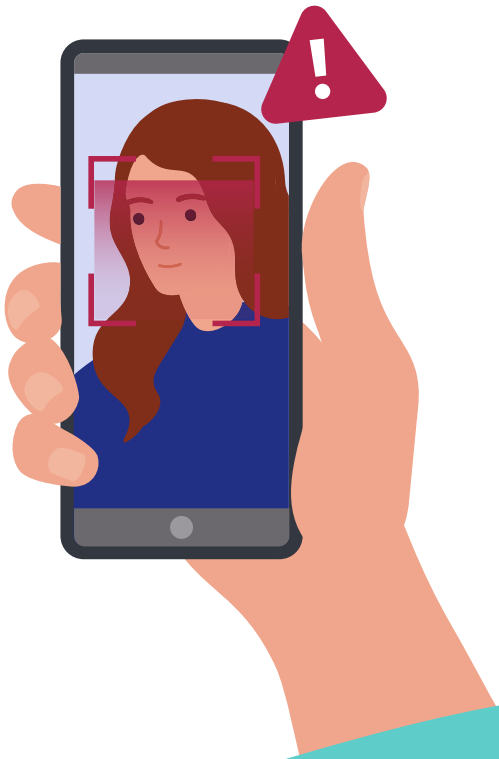
Deepfakes and the law

It's important for young people under 18 to understand that the creation and distribution of nude or sexual deepfakes (even as a misguided joke or meme) can be a criminal offence in some states, as it is for adults across the country. Laws around this kind of behaviour are evolving, and there is increasing legal recognition of the serious harm it can cause. For example, legislation in South Australia criminalises the creation and distribution of AI-assisted deepfakes that are humiliating, degrading, invasive, or sexually explicit, even if the content is entirely synthetic, and the offender is under 18.

Supporting your child

Have non-judgemental, open and ongoing conversations about online experiences. This approach will help them feel safe coming to you if they have issues online. Talk regularly about what's 'real' content and what might be 'fake'. Encourage your child to pause and think before sharing any content – especially when emotions are high.

Include AI in conversations about respectful relationships. This can help develop the awareness, empathy and critical thinking skills your child needs for safe and respectful interactions online. Include discussions about what consent looks like in digital environments. Highlight that creating, sharing or on-sharing nude or sexual deepfakes without consent is a form of image-based abuse that is often extremely harmful.



Tips for dealing with deepfakes

If your child is the victim

1. **Listen and support calmly, without judgement.** It's not the time to criticise or blame as this will increase everyone's stress. Reassure them that it's not their fault and you are there for them.
2. **Support with evidence collection.** Ask your child if they would like support to record information such as URLs, usernames, dates and times of incidents.
3. **Report the deepfakes.** This can be to the platform, to the school if other students are involved, to local police and then to eSafety. You can support them to follow the Reporting Steps (in this summary sheet).
4. **Provide further care and help.** Ask how they feel and what they would like you to do to help – you could suggest it may be helpful for them to talk with someone from a free and confidential counselling or support service such as Kids Helpline.

Use supportive language

Your child may be feeling humiliation, self-blame and even shame. They may also be worried they won't be believed. Use phrases that let them know you're on their side, such as 'This isn't your fault', 'I'm so glad you came to me', 'It took courage to tell me – thank you for trusting me', 'Let's talk to someone who can help.'

Additional advice can be found on the eSafety website: How to help someone deal with image-based abuse.

If your child is sent a deepfake

Unfortunately, encountering harmful content like nude and sexual deepfakes can be part of the online experience for many young people.

Young people want to be able to talk about what they've seen – without the fear of being blamed, criticised or punished. If your child speaks to you about their experience of being sent a nude or sexual deepfake, you could try these conversation starters:

- 'What was your first thought when you saw it?' This helps you connect with their emotions first, rather than just reacting to the situation.
- 'Even if it's fake, someone could be hurt by it.' This starts a conversation about empathy and impact.
- 'Not on-sharing was a really good choice.' This reinforces that they've made a good decision.

If your child created or shared the deepfake

If your child has created and/or shared a deepfake it's time for a conversation – one that may help shape how they understand empathy, respect and responsibility both online and offline.

- Give them the space to explain – avoid jumping to criticism, blame or punishment, for example, ask: 'Can you help me understand how this happened'?
- Explain the serious and harmful impacts – to reputations, mental health and relationships, from the content and from possible legal action.
- Talk about values, not just rules – respect, consent and online responsibility. For example, 'How would you feel if your sister was the subject of these deepfakes?
- Discuss accountability – if possible, help them to apologise, delete or report the content and make amends.
- Set clear boundaries moving forward – develop these boundaries around online behaviour together, with agreed consequences for crossing them.
- Make sure they are OK – even when a young person has done the wrong thing online – address the harm, but keep in mind their age and the complexity of the online world they are learning to navigate.

Additional advice can be found on the eSafety website: **What to do if you shared someone's intimate image or video**.

Reporting steps

If your child is the victim of a deepfake, you can help them by exploring the options for dealing with it. You can support both their wellbeing and their ability to make informed decisions about what happens next. This can include completing the reporting process together.

Possessing sexualised material of under-18s is unlawful so it is best practice, even for parents, to avoid viewing, collecting, printing, sharing or storing nude or sexual content, even if it's fake. A written description of the material can be made and appropriate **evidence** collected, such as the account profiles, usernames, and the web page addresses (URLs). If a deepfake incident involves other students, we recommend contacting a member of the school leadership team as soon as possible and working with them by sharing all relevant information to support a safe and appropriate response.

No matter the circumstance or who else is involved, we recommend making a report to the local police who can provide you with an 'event number' as a record.

You can also **report it to eSafety**, so we can help remove the content online. Provide as much information as possible, including the police event number, so eSafety investigators can assess the situation.

eSafety resources

Deepfakes | What are deepfakes?

Report online harm

How to collect evidence

How to help someone deal with image-based abuse

Managing the impacts of image-based abuse

What to do if you shared someone's intimate image or video

Sending nudes and sexting

Counselling and support services

Parents

The hard-to-have conversations

Webinars for parents and carers

Last updated: June 2025