AI DEEPFAKES

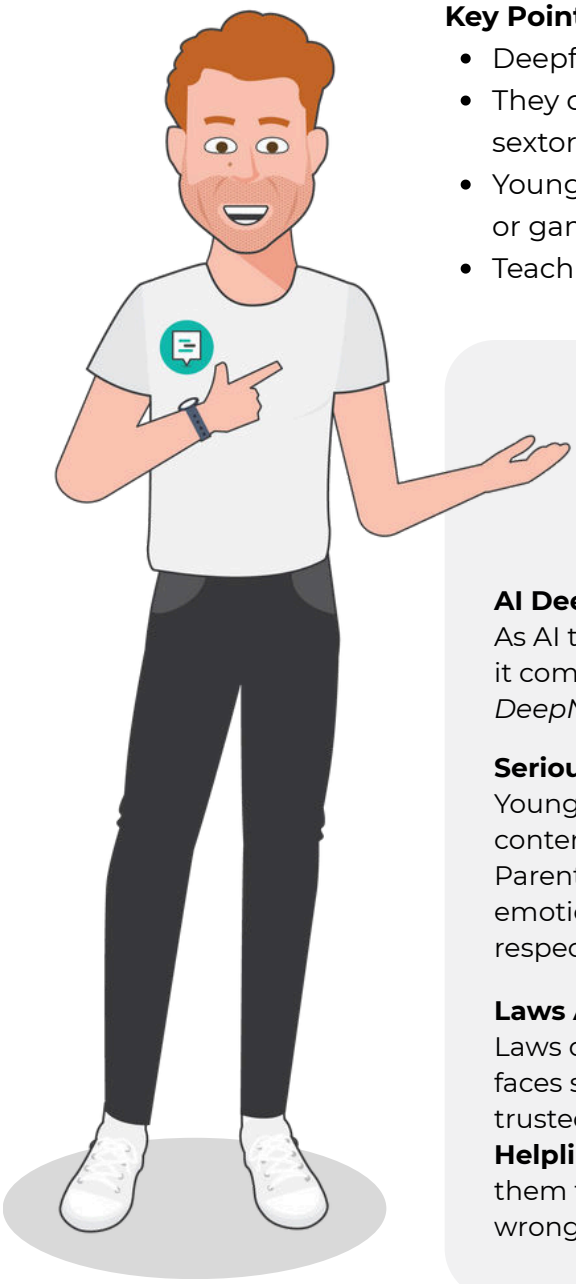
PARENT TOOLKIT

CYBER SAFETY PROJECT

AI DEEPFAKES

"AI deepfakes are reshaping how we see and hear online content. They can be used to mislead, scam, and even exploit — and kids may not realise what's real and what's fake."

— Sam Macaulay -, Cyber Safety Project



Key Points for Parents:

- Deepfakes use AI to create realistic but fake videos, images, or audio.
- They can be used for pranks, misinformation, bullying, scams, and sextortion.
- Young people may encounter deepfakes in social media, group chats, or gaming platforms.
- Teaching kids to question digital content is key to keeping them safe.

WHY YOUNG PEOPLE MUST UNDERSTAND AI LAWS AND DEEPFAKE RISKS

AI Deepfake Risks Are Growing
As AI tools become more powerful, so do the risks — especially when it comes to apps that can create fake, sexualised images like *DeepNudeAI*. These tools are not just unethical, they're illegal.

Serious Consequences for Sharing
Young people need to know that generating or sharing deepfake content, can lead to serious consequences including criminal charges. Parents play a vital role in helping kids understand the legal and emotional harm these tools can cause and in building a culture of respect and responsibility online.

Laws Also Protect Young People
Laws don't just punish, they protect. If a young person or their friend faces sextortion, threats, or deepfake abuse, they should speak to a trusted adult and seek help from the **eSafety Commissioner**, **Kids Helpline** (1800 55 1800), or the police. Knowing where to turn helps them feel safer, more confident, and ready to act if something goes wrong.

Recommended Reading:

- Cyber Safety Project – Understanding AI and Deep Fakes
- eSafety Commission – Deepfake Trends and Challenges
- Common Sense Media – Deepfakes Can Be A Crime

KEY TERMS FOR PARENTS

Knowing the right words makes it easier for you to guide and protect your child online. Here are some key terms you might come across when talking with your child about AI, deepfakes, and online safety.

Artificial Intelligence: Computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Generative AI: Deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.

AI Chat Bot: Dynamic, human-like responses to text prompts using advanced AI models.

Child sexual abuse material (CSAM): shows a sexual assault against a child and can be considered a sub-set of child sexual exploitation material. Child sexual exploitation and abuse material is illegal to create, share or keep.

Child sexual exploitation material (CSEM): is any content that presents a child in a sexual context. It includes content that sexualises and takes unfair advantage of a child, as well as content that shows sexual activity by a child.

Deepfake: A digital photo, video or sound file of a real person that has been edited to create an extremely realistic but false depiction of them doing or saying something they did not actually do or say.

Deepfake image-based abuse: The creation, distribution or threat to distribute fake pornography (CSAM if under 18) without the consent of the person whose face, body or voice appears in the image or video.

Image-based Abuse : The sharing or threat to share intimate images or videos of a person without their consent.

Harmful sexual behaviour (HSB): Sexual behaviours (online or in real life) by children/young people (under 18) that are developmentally inappropriate, may be harmful towards self or others, or be abusive towards another child, young person or adult. When a child under the age of 18 causes sexual harm to another child, this is sometimes referred to as 'harmful sexual behaviour' instead of child sexual abuse.

Online child sexual abuse material: Any form of sexual abuse of a child (under 18) linked to the online environment.

Peer-to-peer sexual abuse: Children (under 18) displaying sexual abusive behaviours towards other children.

SHOW THEM YOU KNOW

Our recent investigation into the habits of young people found that **only 1 in 3 would turn to a parent if something went wrong online**. Showing your child you know a bit about AI is a great way to build their confidence that you're someone they can come to for help. If they see you understand the risks, the steps to take, and where to get help if deepfake scams or abuse happen, they'll know you've got their back.

Here are three trusted places you can take your child online. Use these resources — along with the conversation starters and abuse stories — to kick off a conversation about deepfake safety and how to handle risks together.

Youth Law Australia

Providing free, confidential legal information & help for young people under 25

yla.org.au

eSafety

Cyberbullying, image-based abuse, illegal content.

esafety.gov.au

Take It Down

Help to remove online nude or sexually explicit photos and videos (before you were 18).

takeitdown.ncmec.org

START THE CHAT

THE FAKE PHOTO

AI DEEP FAKE | IMAGE-BASED ABUSE | CSAM

Ella thought it was just another ordinary school day — until a friend whispered that people were passing around a nude photo of her. The shocking part? She'd never taken such a photo. An AI app had been used to edit an innocent picture, making it look disturbingly real. Embarrassed and scared, Ella went straight to her parents. Together with her school, they acted fast: reporting the image, supporting Ella emotionally, and making sure it was taken down. The classmate responsible hadn't realised that creating and sharing such content could lead to serious legal trouble — but they quickly found out.

Chat about:

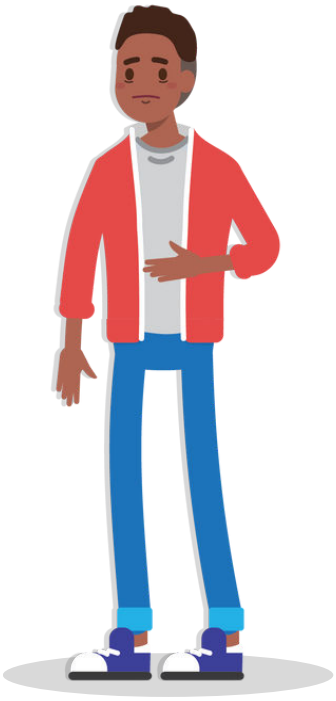
- What would you do if you saw a fake image of yourself or a friend online?
- Who could you talk to right away if something like this happened?
- Why do you think the law treats sharing fake sexual images as seriously as real ones?

REPORT ABUSE | eSafety.gov.au

THE SCAM CHAT

AI DEEP FAKE | BLACKMAIL | SEXTORTION | SCAM

Luca loved chatting about football and gaming on social media. When a new follower started asking about his hobbies, he thought he'd found a genuine friend. But after a few weeks, things took a darker turn — the person used AI to create a fake nude image of Luca from photos on his profile, then threatened to send it to his friends unless he shared more pictures. Shocked and scared, Luca told his parents straight away. They helped him block the account, report it to Instagram and the eSafety Commissioner, and made sure he was safe from further contact. The experience showed Luca how scammers can use AI to make threats feel real — and how speaking up quickly can stop the harm.



Chat about:

- How can you tell if someone online isn't who they say they are?
- What would make you feel comfortable telling me if something online made you uneasy?
- Why do you think scammers target young people through friendly conversation first?
- Would you like to practise the steps to take control of sextortion if it happens to you?

BLOCK USER → REPORT TO APP → CONTACT POLICE → SEXTORTION HELP ACCCE.ORG.AU | 1800 333 000

FREQUENTLY ASKED QUESTIONS

How can I tell if my child might be affected by a deepfake or online abuse?

Look for sudden changes in behaviour — avoiding school or friends, deleting social media accounts, seeming anxious when messages come in, or hiding devices. These may be signs they've seen or experienced something distressing online.

What can I do to reduce the risk of my child's images being misused?

Encourage privacy-smart habits:

- Keep accounts private and limit who can see posts
- Avoid posting close-up face selfies publicly
- Use strong, unique passwords for all accounts
- Consider watermarking original images before posting

How can I help my child spot a deepfake?

AI-generated images and videos can be hard to detect, but common signs include:

- Strange lighting or shadows
- Blurry or distorted hands, jewellery, or backgrounds
- Lip movements that don't match the audio
- Inconsistent clothing details between frames

Is it true that deepfakes mostly target girls?

No, boys can also be targeted, often through scams and sextortion. Scammers may use gaming avatars, sports photos, or social media images.

What should I do if my child is targeted by a deepfake scam or abuse?

- Stay calm and act quickly:
- Save evidence (screenshots, URLs)
- Block the offender and report to the platform
- Contact the eSafety Commissioner or the police
- Offer ongoing emotional support

Can deepfakes be completely removed from the internet?

Not always, but quick action can limit the damage. Report it to the platform, the eSafety Commissioner, and the police if needed. Save evidence before it's deleted — fast reporting reduces harm and helps track offenders.

How can I support my child emotionally after a deepfake incident?

Reassure them they're not to blame, and remind them they're safe now. Encourage open communication. If needed, seek support from Kids Helpline, school counsellors, or parent helplines.

What if the person targeting my child is overseas?

Australian laws still apply if the harm is happening here, but enforcement may take longer. Report to the eSafety Commissioner — they work with international partners to remove illegal content.

Where can I get help right now?

- **eSafety Commissioner:** esafety.gov.au
- **Kids Helpline:** 1800 55 1800
- **Police:** 000 (emergency) or local station
- **Youth Law Australia:** yla.org.au
- **Take It Down:** takeitdown.ncmec.org
- **International support:** inhope.org

SEXTORTION

MYTHS VS FACTS

MYTH: Sextortion is always about money.
FACT: Offenders may also demand more intimate images or videos, threaten to share what they already have, or try to control and humiliate their target.

MYTH: Only girls are victims.
FACT: Boys are also targeted, often for money, while girls are more often pressured for additional images. Both are serious crimes.

MYTH: It only happens between strangers.
FACT: Sextortion can be carried out by people your child knows, including peers, ex-partners, or online "friends".

MYTH: Once the offender gets what they want, it is over.
FACT: Offenders often come back with more threats. Speaking up early is the safest way to stop the harm.