Preventing Deepfakes from causing Real Harm

April 2026

Christians believe human beings are created in the likeness and image of God, and they look to the example of Jesus to live their lives. All the recorded encounters between Jesus and children were kind, gentle and respectful. Children were central to the new social order Jesus initiated.
World Council of Churches, "Helping Children Out of the Shadows and into the Light. Resources for Spiritual Life Addressing Sexual Violence Against Children", May 2020, 4.

As defined by the Australian eSafety Commissioner, a deepfake is:

> *A deepfake is a digital photo, video, or audio 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. Deepfakes are created using artificial intelligence software that currently draws on a large number of photos or recordings of the person to model and create content.*

Deepfakes can be used to cause serious harm, especially when used to create sexually exploitive material of children and adults. In February 2026, UNICEF expressed concern at the increasing use of AI to produce sexualized content involving children. In a UNICEF, ECPAT and INTERPOL study across 11 countries, at least 1.2 million children disclosed having their images manipulated into sexually explicit deepfakes in the past year. In some countries, this represented as much as 1 in 25 children.

In March 2026, the UN expressed concern that deepfake abuse is part of a much broader pattern of digital violence targeting women and girls. They pointed out that sexual deepfake videos make up 98% of all deepfake videos online, and 99% of them depict girls or women.

UNICEF expressed concern that too many AI models are not being developed with adequate safeguards.

In June 2025, the Australian eSafety Commissioner raised concerns that naked deepfakes of students and teachers were an increasing problem at schools. They were being used as a form of bullying or as part of deliberate image-based abuse, causing very real emotional and psychological harm. Victims of deepfake abuse can experience humiliation, shame, distress, fear, anger, and confusion.

The Australian Parliament took an important step by criminalising the non-consensual transmission of AI-generated sexually explicit material via the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth)*. However, regulation gaps remain in relation to sexually explicit deepfake material, and the regulation of non-sexual deepfake material is addressed only indirectly through older laws not designed for AI. Australia's legal framework requires broader reforms to address the full spectrum of deepfake harms.

On 16 February 2026, the NSW *Crimes Amendment (Intimate Images and Audio material) Act* came into effect. It criminalised not just the distribution of sexually explicit deepfake intimate images and audio material, but also alteration and production.

Grok is generating abusive deepfakes at scale
In January 2026, concerns were raised that the Grok AI chatbot on Elon Musk's social media platform X was being used to create and share non-consensual naked images of people and child sexual abuse material. It was reported that Grok was generating 6,700 images of undressed children and adults an hour.

Regulators in several countries, including Malaysia, Indonesia, the UK and Australia, have already taken action against AI technology that can be used to generate sexual deepfakes or are formally investigating Grok's misuse. App stores have already removed AI-nudifying

and undressing apps after evidence showed they were being used to create non-consensual sexualised images of real people, including children. Those removals recognised that this technology-facilitated abuse violates app store policies on sexual exploitation and harassment.

Grok enables the same behaviour, at scale. Yet Apple and Google continue to host the Grok app, applying a different standard despite the documented harm. The same rules that led to the removal of other nudifying apps must be applied here.

What You Can Do

Write polite and respectful letters to:

The Hon Anthony Albanese MP
Prime Minister
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

Salutation: Dear Prime Minister

The Hon Michelle Rowland MP
Attorney-General
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

Salutation: Dear Attorney-General

The Hon Anika Wells MP
Minister for Communications
PO Box 6022
House of Representatives
Parliament House
Canberra, ACT, 2600

Salutation: Dear Minister

Points to make in your letter:

- Express deep concern at the harm deepfakes are causing and that there remain gaps in Australian laws and regulations to deal with the problem.
- Request the Commonwealth Government:
    - To expand the offences on generating sexually exploitive deepfakes, including audio-only depictions and ensure it is an offence to create such material;
    - Require online platform corporations to have a duty of care to proactively detect and remove deepfake material, backed by independent compliance audits and penalties for systemic non-compliance;
    - Require AI models to be developed to be safe by design, including that those that can generate deepfakes have to label the material as deepfake material, so that those viewing or hearing the material know it is a deepfake;
    - Ensure there are standardised national school response protocols to incidents of students using exploitive or abusive deepfakes, building on the eSafety Commissioners Toolkit;
    - Create a Commonwealth survivors of crime compensation scheme for survivors of online child sexual abuse, including survivors of sexually exploitative deepfakes; and,
    - Create offences to address non-sexual deepfakes used for criminal or harmful purposes, such as impersonation for fraud, election interference and fabrication of defamatory “evidence”. There should be aggravated penalties where significant harm is proven.

Please send us copies of any replies you get to your letters to jim@victas.uca.org.au.