How Australia can avoid South Korean schools deepfake crisis

By Joel Scanlan

Australian schools are seeing a growing number of incidents in which students have created deepfake sexualised imagery of their classmates. The eSafety Commissioner has urged schools to monitor the situation.

In 2024, the problem of deepfakes became a crisis in South Korea: more than 500 schools and universities were targeted in a coordinated wave of deepfake sexual abuse.

AI-generated sexualised images of students — mostly girls — were circulated in encrypted Telegram groups. The perpetrators were often classmates of the victims.

A new report from global child-protection group ECPAT, with funding from the UK-based Churchill Fellowship, takes a close look at what happened in Korea, so other countries can understand and avoid similar crises. Here's what Australia can learn.

A glimpse into our future?

The events in South Korea were not just about deepfake technology. They were about how the technology was used.

Perpetrators created groups on the Telegram messaging platform to identify mutual acquaintances in local schools or universities. They then formed "Humiliation Rooms" to gather victims' photos and personal information so they could create deepfake sexual images.

Rooms for more than 500 schools and universities have been identified, often with thousands of members. The rooms were filled with deepfake imagery, created from photos on social media and the school yearbook.

Bots within the app allowed users to generate AI nudes in seconds. One such bot had more than 220,000 subscribers. The bot gave users two deepfake images for free, with additional images available for the equivalent of one Australian dollar.

This wasn’t the dark web. It was happening on a mainstream platform, used by millions.

And it wasn’t just adult predators. More than 80 per cent of those arrested were teenagers. Many were described as “normal boys” by their teachers — students who had never shown signs of violent behaviour before.

The abuse was gamified. Users earned rewards for inviting friends, sharing images, and escalating the harm. It was social, yet anonymous.

Could this happen in Australia?

We have already seen smaller, less organised deepfake incidents in Australian schools. However, the huge scale and ease of use of the Korean abuse system should be cause for alarm.

The Australian Centre to Counter Child Exploitation recorded 58,503 reports of pictures and videos of online child abuse in the 2023–24 financial year. This is an average of 160 reports per day (4,875 reports a month), a 45 per cent increase from the previous year.

This increase is likely to continue. In response to these risks, the Australian government, through the eSafety Commissioner, is applying the existing Basic Online Safety Expectations to generative AI services. This creates a clear expectation these services must work proactively to prevent the creation of harmful deepfake content.

Internationally, the European Union’s AI Act has set a precedent for regulating high-risk AI applications, including those that affect children. In the United States, the proposed Take It Down Act aims to criminalise the publication of non-consensual intimate images, including AI-generated deepfakes.

These are a start, but a lot more work remains to be done to provide a safe online environment for young people. The Korean experience shows how easily things can escalate when these tools are used at scale, especially in peer-to-peer abuse among adolescents.

Five lessons from Korea

The South Korean crisis holds several lessons for Australia.

1. Prevention must start early. Korea’s crisis involved children as young as 12 (and even younger in some primary schools targeted). We need comprehensive digital ethics and consent education in primary schools, not just in high schools.
2. Law enforcement needs AI tools of their own to keep up. Just as offenders are using AI to scale up abuse, police must be equipped with AI to detect and investigate it. This may include facial recognition, content detection and automated triage systems, all governed by strict privacy protocols.
3. Platforms must also be held accountable. Telegram only began cooperating with South Korean authorities after immense public pressure. Australia must enforce safety-by-design principles and ensure encrypted platforms are not safe havens for abuse.
4. Support services must be scaled up. Korea’s crisis caused trauma for entire communities. Victims often had to continuing going to school with perpetrators in the same classrooms. Australia must invest in trauma-informed support systems that can respond to both individual and collective harm.
5. We must listen to victims and survivors. Policy must be shaped by those who have experienced digital abuse. Their insights are crucial to designing effective and compassionate responses.

The Korean crisis didn’t happen overnight. The warning signs were there: in 2023 Korea produced more than half the world’s celebrity deepfakes. This has been accompanied by rising misogyny online and the proliferation of AI tools. But they were ignored until it was too late. Australia mustn’t make the same mistake.

Joel Scanlan is a senior lecturer in health information management at the University of Tasmania. The opinions expressed in this article are that of the author and do not necessarily reflect any official policies or positions of the AEU or SSTUWA.
This article was first published on The Conversation website and has been reproduced here with permission.

THE CONVERSATION

Authorised by Mary Franklyn, General Secretary, The State School Teachers' Union of W.A.

ABN 54 478 094 635 © 2025