Modern slavery risks in the higher education sector

Artificial Intelligence

THE UNIVERSITY OF SYDNEY

78% of students (tertiary and school) have recently used a generative AI tool.[1]

32% of businesses expect a decrease in their workforce in the next year as a result of AI, according to a survey of close to 2,000 professionals.[2]

US$4.8 trillion is the expected global market share for AI in 2033.[3]

What is modern slavery?

Modern slavery is a serious violation of an individual's dignity and human rights. Exploitative practices, including human trafficking, forced labour, child labour, debt bondage and forced marriage, are all considered modern slavery and are serious crimes under Australian law.

Regulatory context

Modern Slavery Act 2018 (Cth)

Organisations, including universities, based or operating in Australia with at least AU$100 million in annual consolidated revenue are required to report annually on the steps they have taken to identify and address modern slavery risks in their operations and supply chains. See *Commonwealth Modern Slavery Act Guidance for Reporting Entities*.

Modern Slavery Act 2018 (NSW)

Certain universities in NSW have due diligence reporting obligations under the NSW Modern Slavery Act to ensure the goods and services they procure are not the product of modern slavery. See *NSW Anti-slavery Commissioner's Guidance on Reasonable Steps to Manage Modern Slavery Risks in Operations and Supply-Chains*.

Modern slavery practices in the AI sector

Human Trafficking

Generative AI is being exploited by transnational criminal organisations to create sophisticated, multilingual personas and scams, enabling deceptive recruitment and human trafficking across borders and at a greater scale globally.

Forced Labour & Child Labour

AI training, involving data annotation, analysis and verification, relies on significant outsourced labour, reported to work in exploitative conditions, including underpayment of wages, excessive hours and exposure to psychological harm. Indicators of forced labour and child labour have been reported in the AI supply chain.

Child Exploitation

AI has been used to enable the creation and circulation of exploitative content involving children online. For example, recommendation systems, used by social media platforms to suggest content or connections, are shown to have enabled child grooming. Generative AI is being used to create large amounts of synthetic child sexual abuse material.

Why is the sector high risk?

Increased economic and social vulnerability

Automation displaces low-skilled workers, increasing competition for diminishing supply of work and leaving them in precarious situations, which may pressure them to take on work in exploitative conditions.

Limited regulatory frameworks

Inadequate regulation that fails to keep up with the rapid pace of AI and a reliance on non-binding principles creates gaps in the governance and accountability of AI development and application.

[1] Case study: The AI Divide in Australia, Australian Digital Inclusion Index, 2025

[2] The state of AI in 2025: Agents, innovation, and transformation, McKinsey & Company, 2025

[3] AI market projected to hit $4.8 trillion by 2033, emerging as dominant frontier technology, UN Trade & Development, 2025

Modern slavery risks in the higher education sector

Artificial Intelligence

THE UNIVERSITY OF SYDNEY

How modern slavery and human rights risks in the AI sector may be linked to universities

Procurement *Universities may be linked to modern slavery risks or human rights risks in the AI sector through their supply chains, including in the manufacturing of electronic components, final assembly of products and in the labour to deliver services on campus.*	
Product, Sector & Geographic Risks	Sourcing AI software without adequate due diligence of the supplier or application: • **AI for research and information management** often relies on outsourced labour to train AI algorithms and moderate content. Workers have reported insecure and low paid conditions, fear of speaking up, traumatic exposure to harmful content and indicators of forced labour *(e.g. workers in Africa supporting AI functions for social media and chatbots exposed to "inhumane working conditions").* • **AI for surveillance and campus safety** may violate staff and student privacy or be inadvertently used to undermine freedom of expression. • **AI-related electronics**, such as servers, specialised processors and other hardware for high-performance computing or research labs, may be linked to forced labour and child labour in the electronics supply chain. • **Failure of AI systems for payroll, admissions, and student management** can lead to financial harm, legal liability and reputational concerns *(e.g. failure of AI systems in Australia's unlawful debt recovery scheme).* • **AI for staff recruitment, student admissions, automated grading, or scholarship allocation** may perpetuate discrimination and exclusion of vulnerable groups, through algorithmic bias *(e.g. AI-powered recruitment platform sued over allegations it discriminates, based on age, race and disability).*
Teaching & Research *Universities may be linked to modern slavery risks, through their teaching and research activities and partnerships. Risks often intersect with other human rights concerns and counterparty risks related to sensitive technologies, sanctions and national security.*	
Research Development & Application Risks	Research without adequate due diligence of the partner, design or application: • **AI research in high risk locations** with frequent reports of AI-related harm and limited regulation increases the likelihood of ethical breaches, such as inadequate privacy protections or unsafe testing. • **Continuous training of AI human and image-generators** with live, unvalidated data streams risks data poisoning, where the malicious or biased data is introduced, resulting in potentially harmful applications of the research, such as generation of child sexual abuse material or misinformation. There is a risk that workers engaged in AI data labelling may be coerced to carry out foreign interference or corruption of AI. Research with dual academic and commercial use without adequate due diligence: • **AI-enabled surveillance technologies, such as facial recognition software, emotion-detection tools and profiling systems** may be inadvertently used for human rights and labour rights harm, with reports of AI technologies used to track ethnic minorities, violate the privacy of workers through intrusive monitoring and censor and repress citizens *(e.g. Australian university researcher's facial recognition software to identify ethnic minorities in Chinese-government funded project).* • **Developments in generative AI** may inadvertently enable creation and sharing of hyper realistic explicit content, including child sexual abuse, violent and extremist material.
Partnership & Collaboration Risks	**Partnering with AI companies with links to human rights violations:** • The U.S. has sanctioned several technology firms for development of AI-enabled surveillance software involved in the monitoring and repression of ethnic minorities *(e.g. U.S. sanctions China's largest facial recognition start up)* • Australian universities have faced criticisms for collaborations linked to potential misuse of AI for human rights harm.

Modern slavery risks in the higher education sector

Artificial Intelligence

Case study

This case study has been developed using publicly available reports. It is intended solely for illustrative purposes and does not represent any specific university, supplier, or partner organisation.

An Australian University, with a strong reputation in artificial intelligence research, partnered with a private tech startup to develop advanced facial recognition algorithms intended for public safety applications.

The University's researchers worked with the partner to develop enhancements to identify in real time across large crowds. While the technology was initially tested in controlled environments, after the project commenced the private partner, who owned the IP, commercialised it and sold it to foreign governments and third-parties.

Several years after the research, the University was named in a media article on the use of the technology for tracking journalists and human rights defenders, some of which were harassed and imprisoned unlawfully.

Learn more

- Scroll. Click. Suffer: The Hidden Human Cost of Content Moderation and Data Labelling, equidem, 2025
- Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias, Australian Human Rights Commission, 2020
- The use of Generative AI to facilitate trafficking in persons, OSCE, 2024
- Algorithmic Accountability Toolkit, Amnesty International, 2025
- Salient Issue Briefing: Artificial Intelligence-based Technologies, Investor Alliance for Human Rights,
- Generative AI and Child Safety, Australian eSafety Commissioner, 2025

This resource is provided for your general information only and is not a replacement for individual advice that is tailored to your needs. Users of this resource requiring or seeking such advice are responsible for obtaining that advice from their lawyers or other professional advisors. They should do so before taking (or refraining from taking) any action in reliance on any information contained in the resource.