LK

LK Education Insights

Privacy Law Update

Recent and upcoming developments in Australian privacy law signal a significant uplift in regulatory expectations, compliance obligations, and potential liability for organisations handling personal information. For education providers who routinely collect, use and store sensitive student, family and staff data, these reforms and cases underscore the importance of embedding privacy into both governance and daily operations.

Legislative Reforms: Strengthening Australia's Privacy Framework

Following the release of the Australian Government's response to the Privacy Act Review Report in September 2023, the Australian Government has brought several of the proposed reforms into law.

The Privacy and Other Legislation Amendment Bill 2024 (Cth), which received Royal Assent on 10 December 2024, marked the first tranche of Australia's broader privacy law reform. These amendments represent the first steps in enhancing privacy protections and enforcement mechanisms under the *Privacy Act 1988* (Cth) (**Privacy Act**).

The key changes introduced in this first tranche include:

Reform	Implications	Commencement
Data Security, Retention and Destruction	APP entities must take both technical and organisational measures to secure, destroy or de-identify personal data.	Commenced 11 December 2024
Criminalisation of Doxxing	It is now a criminal offence to publish personal data online in a menacing or harassing way.	Commenced on 11 December 2024
Tiered Penalties and Enforcement	OAIC gains new investigative powers, compliance notices, and a tiered civil penalty regime.	Commenced on 11 December 2024
Statutory Tort for Serious Invasions of Privacy	Individuals may sue for intentional or reckless serious invasions of privacy, without needing to prove loss.	Commenced on 10 June 2025
Automated Decision-Making Disclosure	Privacy policies of APP entities must disclose use of AI or automated systems in decisions significantly affecting individuals.	From 10 December 2026
Children's Online Privacy Code	Will specify how privacy principles apply to online services accessed by children.	From 10 December 2026 (Draft and Explanatory Statement published 31 March 2026. Public consultation closed 5 June 2026)

Expected reforms on the horizon

Some of the most significant proposed reforms that were agreed to or agreed to in-principle by the Australian Government have yet to be tabled including many of those that are set to have the biggest impact on organisations.

These potential reforms include:

- enhanced definitions of key concepts in the Privacy Act, including 'personal information', 'collection' and 'disclosure';
- the removal of the small business exemption, bringing organisations with an annual turnover of $3 million or less under the Privacy Act;
- a new objective 'fair and reasonable' test for the collection, use and disclosure of personal information (irrespective of whether consent has been obtained);
- privacy policies and collection notices likely to be subject to specific requirements;
- cross-border data transfers will be facilitated through an adequacy regime, with appropriate protection mechanisms;
- enhanced control and rights for individuals in relation to personal information held by entities, including rights regarding access, correction, objection, erasure and withdrawal of consent;
- further organisational accountability measures including appointing / designating a senior employee with specific responsibility for privacy;
- a further direct right of action for individuals for breaches of the Privacy Act; and
- potentially enhanced protections for employees.

In January 2026, the OAIC conducted its first ever privacy compliance sweep. The OAIC targeted entities in 6 sectors that generally collect information in-person (for example, rental and property, car rental and dealership and pharmacy sectors). The sweep focussed on the review of privacy policies of approximately 60 entities in these sectors for compliance with the requirements under the Australian Privacy Principles (**APPs**).

Privacy Law Developments in the Courts: Penalties and Claims

First civil penalty proceeding – Australian Clinical Labs

In the first civil penalty proceeding under the Privacy Act, the Federal Court ordered Australian Clinical Labs (**ACL**), one of Australia's largest pathology services providers, to pay $5.8 million following a 2022 data breach that exposed the health and other personal information of over 223,000 individuals.

The Court's decision provides useful guidance on what does and does not constitute 'reasonable steps' under APP 11.1 and what is expected of organisations subject to the requirements of the Privacy Act when a data breach occurs, including that:

- ACL's failure to implement adequate cybersecurity controls (including encryption, multifactor authentication, suitable anti-virus software and effective internal procedures and training) constituted a failure to take reasonable steps to protect personal information.
- ACL failed to conduct a timely and adequate assessment of the suspected data breach, placing unreasonable reliance on advice from a third-party provider that no individual was harmed because of the breach after a limited investigation.
- ACL did not notify the OAIC 'as soon as practicable' of the eligible data breach, waiting several weeks despite clear indicators that personal data may have been compromised.

The Court found each contravention was 'serious' under s13G of the Privacy Act, noting the sensitivity of health data and ACL's failure to act diligently.

While the agreed penalty was well below the theoretical maximum (with the Court accepting that ACL had committed 223,000 contraventions of APP 11.1), ACL was still required to pay a significant penalty of $5.8 million as a consequence of the breaches.

This decision highlights that data protection obligations under APP 11 require that organisations ensure strong cybersecurity measures are in place proportionate to the sensitivity and volume of data, including appropriate and robust technical and organisational measures (such as internal response procedures, staff training and designating responsible persons).

Organisations subject to the Privacy Act are also required to act swiftly in response to any suspected data breaches, ensuring that they conduct a timely and adequate assessment of whether the data breach is an 'eligible data breach' (i.e. a data breach that is likely to cause serious harm to an individual) and therefore reportable to the OAIC. The ACL penalty demonstrates that reliance on third party advice may not be sufficient for the purposes of conducting this assessment.

First claims under the new statutory tort for serious invasion of privacy

In August 2025, the Federal Court saw the first claim filed for serious invasion of privacy, by the Victorian Deputy Liberal Leader and his wife against the Herald Sun, an editor and journalist. The plaintiffs alleged that an article about their relationship was both defamatory and constituted a serious invasion of privacy.

To establish a claim for serious invasion of privacy, a claimant must show intentional or reckless intrusion or misuse of private information, a reasonable expectation of privacy, and that the invasion was serious. The Court will also be required to weigh whether the public interest in privacy outweighs competing interests such as freedom of expression or open justice.

The proceedings, which were set to become the first test case of the statutory tort, settled out of court in November 2025, with the Herald Sun publishing an apology to the plaintiffs.

Separately, in October 2025, the District Court of New South Wales granted an interlocutory injunction, the first of its kind concerning an alleged serious invasion of privacy.

Mr Williams, the respondent, was opposed to a development application lodged by the first applicant, Kurraba, with the City of Sydney. Following unsuccessful negotiations between the parties, Mr Williams began a campaign against the second applicant, Mr Smith (CEO of Kurraba) which, amongst other things, included Mr Smith's private wedding photographs being published on the internet.

The judge found that the wedding photographs were never intended to be made public, in circumstances where Mr Smith and his wife were not public figures and the photographs were misused by Mr Williams, whose conduct was characterised as an extortion and not a journalistic style investigation.

The Court found that there was a serious question to be tried in relation to the tort of privacy and granted interlocutory injunctions against Mr Williams, restraining him from publishing any further material in relation to the plaintiffs or the development, and requiring the removal of such materials from the internet and social media platforms.

Practical Steps Your Organisation Can Take Now

The first tranche of reforms, the next round of expected reforms on the horizon and the increased risk of privacy-related litigation means that organisations should be taking immediate steps to strengthen their data governance and privacy compliance systems. This includes the following:

- Undertake an inventory of the data and digital assets (and liabilities) held by your organisation.
- Review your organisation's collection practices – identify the types of personal information and sensitive information that is collected from students, parents and staff and its purpose (including any secondary purpose). Relevant types of personal information that may be collected may include:
    - Full name
    - Contact details
    - Birth certificate
    - School reports / academic results
    - Education details
    - Payment and billing information
    - Citizenship, residency and visa status and details
    - CCTV footage

- Sensitive information (which is subject to stricter rules relating to use and disclosure) that may be collected, may include:
    - Race, ethnicity, cultural background
    - Religious beliefs or affiliations
    - Sexual orientation
    - Health records and behaviour and wellbeing records

- Consider whether such collection is proportionate to the required purpose, whether there are other ways of achieving that purpose, and whether collected information could satisfy that same purpose if it were de-identified.

- Ensure that your organisation's systems are capable of easily and quickly retrieving, deleting or de-identifying personal information, and take action to permanently erase personal information that is no longer needed or required by law to be retained (to minimise harm from any data breach).

- Ensure that privacy policy and collection notices are clear, up to date and subject to regular review, and implemented and adhered to in practice. Ensure privacy policies clearly disclose automated decision-making and digital platform use that may impact students, families and staff.

- Review the extent to which personal information is disclosed outside the organisation and the data protection, cybersecurity and privacy practices of third parties with whom it is shared. Review contracts with IT and cloud service providers to ensure they meet required technical and organisational safeguards – in particular, ensure that these include any required contractual terms (such as minimum security standards to be met by suppliers, and data incident and indemnity clauses).

- Keep records to ensure that you can prove compliance with current laws.

- Invest in, and regularly review, data governance, cybersecurity and incident response frameworks.

- Ensure that relevant roles and responsibilities throughout the organisation are clearly defined and understood. Ensure that staff know when and how to report data breaches internally and if required, to the OAIC, and that regular training and drills are undertaken.

- Ensure that there is appropriate and meaningful oversight, including monitoring at board level and regular reporting.

- Carefully review operations and determine whether your organisation's activities will bring it within the territorial scope of the European Union General Data Protection Regulation or the United Kingdom General Data Protection Regulation and the *UK Data Protection Act 2018*. This may occur if your organisation enrols or markets to students located in the UK or EU offers online courses or services to individuals in the UK or EU, monitors the behaviour of individuals located in the UK or EU or has an establishment, partnership, or research presence in the UK or EU. If the EU or UK GDPR applies, additional and more stringent obligations may arise, including enhanced transparency requirements, lawful basis assessments, data protection impact assessments, appointment of a UK or EU representative (in some cases), and significantly higher regulatory penalties.

If you would like to discuss these issues further or would like assistance in reviewing your privacy policies and procedures, please get in touch with our team.

Key Contacts



Contact Us

Australia
Level 23, 25 Grenfell Street
SA 5000, Australia
Phone: +61 8 8239 4600

London
33 Black Friars Lane
London EC4V 6EP, United Kingdom
Phone: +44 20 7400 2180



Principal

E acooper-boast@lk.law
T +61 8 8239 4615

Amy Cooper-Boast

Amy has over 20 years of experience litigating commercial disputes and resolving legal and strategic risks and challenges for her clients. She has deep experience in commercial and financial disputes, director and auditor liability, employee misconduct, regulatory inquiries, insolvency and restructuring, and misuse of data, confidential information and IP.

Amy also advises on complex regulatory and compliance issues, including privacy, data governance, whistleblowing, critical infrastructure and sector-specific regulation. Clients appreciate her strategic approach, her excellent legal and analytical skills, her ability to quickly grasp complex industry issues, and her tenacity and steady hand in resolving their sensitive disputes and regulatory concerns.



Principal

E bhall-carney@lk.law
T +61 8 8239 4687

Brooke Hall-Carney

Brooke is a trusted advisor to boards, executives, CEOs and general counsel navigating the intersection of technology, risk and regulation. With deep experience in digital transformation, data protection, governance, cybersecurity including incident response, and global privacy compliance, including advising a US institutional bank in relation to an inadvertent data spill. Brooke also advises clients on the emerging challenges of AI — from regulatory compliance and governance frameworks to model and vendor risk. Brooke is an experienced commercial litigator and technologist who has worked on the mega litigations of Bell, One.Tel and C7.

Brooke is a recognised leader for her work at the intersection of cyber and AI governance. She was shortlisted in Euromoney Asia Women in Business Law Awards Privacy & Data Protection 2018; Doyle's Guide 2017, 2022, 2023, 2024, 2026; Lawyers Weekly Tech Partner 2022; Cyber Partner 2023, 2024; and Australian Cyber Security Awards Cyber Lawyer 2024, 2025 and Australian AI Awards Female Leader SME 2025. Brooke is a member of the AICD (GAICD) and a director on Boards, including a large independent school. Brooke was the recipient of a Commonwealth Fellowship to teach and study a Master of Laws at the University of British Columbia and completed at Harvard, Cyber Security and AI at MIT Sloan in the USA.



Special Counsel

E slo@lk.law
T +61 8 8239 4671

Stephanie Lo

Stephanie is experienced with significant commercial and financial disputes, including matters arising from corporate collapses in Australia and internationally and major construction projects. She has extensive experience advising on issues such as breach of contract, directors' duties, audit negligence, construction defects, professional negligence, corporate governance and fraud. Stephanie also advises clients on privacy law and corporate governance compliance and regularly presents on AI.