brennan law partners

BLP BRIEF

The Privacy Laws & Australian Privacy Principles: A Guide for Schools

April 2018

By Tyson Brennan

On 12 March 2014 significant amendments were made to Australia's privacy laws. The changes are such that they impact upon Non-Government Schools and how they handle personal information. The *Privacy Act 1988* (Privacy Act) protects personal information.

The Federal Privacy Commission now has new investigatory and enforcement powers when dealing with matters of privacy and information use and storage. The Commission also has the ability to hand out significant penalties to organisations that are found to be in breach of the privacy laws.

Therefore, it is now more important than ever to ensure your school's policies and procedures are compliant with the new laws. Not only is compliance crucial to avoid penalties but also to protect your school's reputation.

Who is affected?

The laws apply to all Non-Government Schools *unless* they have an annual revenue of less than $3 million and they do not provide a health service.

All schools hold personal information of thousands of people. Personal information is information or an opinion that identifies a person or could identify them. This can include names and addresses, financial and billing information, and health information. With so much information held by Schools and regular threats to cyber security, the risk of breaching the privacy principals is real for all schools.

The changes

The new laws introduced 13 Australian Privacy Principles (**APPs**) that set out how schools must handle personal information.

Schools must have procedures, practices and systems to ensure compliance with these principles. Schools must also have relevant protocols in place to manage queries and complaints.

The APPs

The relevant privacy laws protect personal information that is "recorded" by an

organisation. Information that is not recorded will likely fall outside the application principals set out below.

APP 1: Open and Transparent Management of Personal Information

Under the new laws, schools have greater responsibility to manage information in an open and transparent way.

Schools are required to implement (and keep updated) practices, procedures and systems to facilitate compliance with each of the APPs.

A school must have a clearly expressed and up-to-date privacy policy explaining what personal information is used and what they do with it and have this available on their public website.

APP 2: Anonymity and Pseudonymity

Individuals have the right to withhold their identity or use an alias when dealing with a compliant school. Schools should ensure that when a request for anonymity is made, relevant practices are in place to ensure the request is complied with.

APP 3: Collection of Solicited Personal Information

A school must not collect personal information unless it is reasonably necessary. "Sensitive information" may only be collected when the individual consents.

APP 4: Dealing with Unsolicited Information

Where the school receives information they did not ask for, the school may keep it only if it was possible to have been obtained in compliance with APP 3.

APP 5: Notification of the Collection of Personal Information

The school must take reasonable steps to notify the affected individual of the purpose and circumstances for the collection as soon as practicable.

APP 6: Use or Disclosure of Personal Information

Information can only be used or disclosed for the purpose for which it was collected. With consent, a secondary purpose may also be allowed.

APP 7: Direct Marketing

It is always best to get consent when it comes to marketing purposes. If this is impractical, an "opt out" facility should be made available.

APP 8: Cross-Border Disclosure of Personal Information

A school must take reasonable steps to ensure any overseas recipient (such as a cloud provider) does not breach the AAPs. The school could be legally accountable if the overseas recipient mishandles the supplied personal information.

APP 9: Adoption of Government-Related Identifiers

A school must not use government-related identifiers for individuals.

APP 10: Quality of Personal Information

Information used, collected or disclosed should be up to date, correct, complete and relevant.

APP 11: Security of Personal Information

Reasonable steps must be taken to ensure personal information is secure and protected from misuse.

Information no longer required must be destroyed.

APP 12: Access to Personal Information

In most cases, a school must grant an individual access to their own personal information if requested.

APP 13: Correction of Personal Information

Reasonable steps must be taken to ensure correction of any out of date, incomplete or inaccurate material held.

If the school has disclosed the material to a third party, they should also be notified of any amendments made.

Who's rights? The parent or the child?

The Privacy Act does not differentiate between adults and children. As your enrolment contract is between the school and the parent it would be a foreseeable position that a parent can act on behalf of their child.

It should be emphasised, however, that children do have rights under the Privacy Act, and in some situations it may be appropriate to seek the child's consent. Where a child seeks to have their personal information withheld from their parents, the school should think carefully about the appropriate decision, considering the individual circumstances.

How can Brennan Law Partners assist?

If you have any concerns about your policies or procedures please contact us to conduct a review for you. Even if your school does not fall within the scope of the Privacy Act, it is wise to have systems in place to protect private information.

If you have any questions regarding any information in this BLP Brief, we welcome you to contact us at any time.

This is meant as a guide only.