Strategic Responsive Solutions

CHANGES TO THE *PRIVACY ACT 1988* (Cth): IMPLICATIONS FOR SCHOOLS

A paper to be presented on 5 December 2013

Educate Plus Queensland Professional Development, B

Author
Alistair Macpherson, Director
Nina Brewer, Graduate Law Clerk
Alistair.Macpherson@corneyandlind.com.au

Level 4, Royal Brisbane Place
17 Bowen Bridge Rd Herston Q 4029
Phone: (07) 3252 0011
Fax: (07) 3257 7890
www.corneyandlind.com.au

Introduction

Privacy law is the law around the collection, storage and use of personal information about individuals by government agencies and businesses. It is governed by the *Privacy Act* 1988 ("**Privacy Act**") and the National Privacy Principles. Many of you would be aware of the Act and have implemented Privacy Policies in compliance with it.

On 23 May 2012, legislation was introduced to Parliament proposing to amend the current *Privacy Act* 1988. This is the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* ("**Privacy Amendment Act**"). It was passed by Parliament (with amendments) on 29 November 2012[1]. A total of 197 changes have been made to the existing Privacy Act.

The changes introduced by the new legislation will come into effect on 12 March 2014. There will be no transition period for these reforms. This means that up to and including 11 March 2014, existing Privacy laws will apply. From 12 March 2014, the new amended Privacy laws will apply. It therefore is very important for schools and businesses to prepare prior to this date by having their existing privacy policies and procedures reviewed to ensure that they have implemented correct processes and policies in order to comply with the incoming legislation.

What's changed?

I will go through some of the most basic changes in Privacy Law, which will give context to the terms used throughout the remainder of this presentation.

All Schools collect information about their students and families to fulfil their obligations to students and their parents. This information is categorised into "personal" and "sensitive" information:

Personal information is information that enables a School to identify an individual. This includes general information such as name, date of birth etc.

Sensitive information is subject to stricter rules of disclosure and is information of a more personal nature, such as sexual preference and political opinions. Medical information is classified as sensitive information. The definition of sensitive information has not changed significantly, and includes:

[1] Australian Government, *Privacy Law Reform* (2013) Office of the Australian Information Commissioner <http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform>.

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

Schools will always handle personal and/or sensitive information and are therefore subject to the new Australian Privacy Principles and must make sure that these principles are complied with.

The types of information schools can be expected to collect in performance of its general functions are:

Students: Full name, birth certificate, medical information, medical reports, race, religion and school reports;

Parents: Full name, marital status, race, religion, contact details;

Staff: Full name, race, religion, tax file number, education details.

There have been various rules in place regulating the collection, use and disclosure of this information. These rules do change under the Australian Privacy Principles. Additionally, there is more scope for a School to be penalised for breaching the rules.

New definition of personal information

As its basic function, the Privacy Amendment Act intends to streamline the handling of personal information by both government agencies and businesses.

The Privacy Amendment Act[2] changes the definition of personal information from *"information about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion"*, to *"information about an identifiable individual or an individual who is reasonably identifiable."* (emphasis added)

That is, it no longer requires the actual identification of the individual but rather the ability to identify the individual if required.

If information that was legally obtained and held by Schools under the NPP's does not comply with the new rules being imposed by the APP's on 12 March 2014, it must be de-identified[3].

The new APP's regulate the handling of personal information.

New definition of sensitive information

The definition of sensitive information will now include information about a person's biometrics, which includes physical and behavioural identifiers such as fingerprints, DNA and voice recognition[4].

"Sexual preferences" has been changed to "sexual orientation"[5].

It will continue to include all other elements of the current section 6(1) definition of the Privacy Act, including racial or ethnic origin, political opinions, religious beliefs and affiliations, and criminal record.

[2] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 36.
[3] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 14.
[4] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 42.
[5] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 41.

Sensitive information is given heightened protection in the Privacy Amendment Act. More stringent requirements are put in place for the collection, storage and use of sensitive information than that of personal information.

Use and disclosure of personal and sensitive information – new Australian Privacy Principles

The Privacy Amendment Act implements a new set of Privacy principles to regulate the handling of personal and sensitive information by government agencies and businesses. These are the Australian Privacy Principles ("**APP's**") which will apply to Schools. They will replace the current National Privacy Principles ("**NPP's**") that currently apply to all Schools.

It will usually be mandatory for Schools to comply with the new Australian Privacy Principles. The APP's set out the minimum standard for the collection, use, disclosure and access to personal and sensitive information of individuals.

There are 13 new APP's. Many of these APP's are different from the existing NPP's, so it is important that Schools become acquainted with these new principles before 12 March 2014 so they can ensure compliance and, as at that time, are legally holding the personal and sensitive information in their possession.

1 NEW ENROLMENTS AND CURRENT ENROLMENTS

New enrolments and current enrolments necessarily require the collection of information from students and their parents or guardians. This may be so that the School can exercise an adequate duty of care to their students, meet their contractual obligations to educate the student (or decide if it is unable to educate the student), record academic results against a student's profile, or to identify students for the purpose of disciplinary action. This part will cover the requirements around the collection and storage of this information.

As of 12 March 2014, there will be new rules that will apply to the collection procedures and notices to be given when collecting personal information and/or sensitive information. Much of this information is collected when students are initially enrolled at a School. However, additional information is also periodically collected (or updated) from students who are currently enrolled at a School.

APP 3: Collection of solicited personal information

Information is solicited if the School takes active steps to acquire it from an individual, or specifically requests it from another entity. This APP governs when and how a School may collect personal information.

Much of the personal information that a School will hold about a student will be acquired upon enrolment, however, during the course of enrolment, schools will be continually collecting personal information. This could be by way of requiring an individual to fill out a form, requesting an individual to give out specific information or, in the case of already-enrolled students, a letter sent home to School families requesting information about the student. All of this information will be solicited personal information.

The collection of personal information has different standards to the collection of sensitive information.

Collection of Personal information

Schools must only collect personal information that is reasonably necessary for one or more of the School's functions or activities[6]. The School's functions or activities will generally relate to the education of the student, so the collection of the person information must be reasonably necessary to that function. Obviously this would include personal details regarding the student. It could also include details regarding their parents and guardians. However, the link can quickly become tenuous, and care needs to be taken.

Collection of Sensitive information

The real risk to Schools relates to the collection of Sensitive Information. The APP's now make it clear that Sensitive Information can only be collected with the consent of the individual concerned (whilst this principle was addressed in the NPP's, there was inconsistency between NPP 1 and NPP 10 in this regard).

The collection of sensitive information is subject to higher protections, as the School cannot collect information of this kind unless the individual consents to the collection and the information is reasonably necessary for one or more of the School's functions or activities[7].

A School may collect sensitive information in the absence of consent where:

[6] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, APP 3.2.
[7] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, APP 3.3(a)(ii).

- It is required or authorised by a court/tribunal;
- A permitted general situation exists;
    - Lessening or preventing a serious threat to life, health or safety;
    - Suspected unlawful action or serious misconduct;
    - Locating a missing person;
    - Establishing, exercising or defending a legal or equitable claim;
    - Where it is reasonably necessary for a confidential alternative dispute resolution process;
    - Necessary for a diplomatic or consular function/activity; and
    - Necessary for Defence Force activities outside Australia;
- A permitted health situation exists (providing a health service or conducting research);
- For an enforcement activity;

The permitted General Situations will be of limited assistance to Schools.

Functions and activities

In order to determine whether the collection of information is necessary for the School's functions as activities, it is necessary to first identify the School's functions and activities. They will generally be described on the School's website, in brochures and in advertising. For the collection of information to be 'reasonably necessary for' the School's functions and activities, the School must establish that a reasonable person would believe that the collection of that information is reasonably necessary for the School's functions or activities. An objective test to consider is whether the School would be able to undertake their functions and activities without that information, or with a lesser amount of that information.

Means of collection – Collecting directly from an individual and obtaining consent

This APP may be problematic in that much of the information collected is about students who are under the age of 18 years. Generally the parent or guardian of a student will supply the information to the School. However, under APP 3.3, an individual must consent to the collection of sensitive information about themselves.

A School must therefore collect personal information about an individual only from the individual unless:

- The individual consents to the collection of the information from someone other than the individual;
- The School is required or authorised by law to collect the information from someone other than the individual; or
- It is unreasonable or impracticable to do so (for example, in the case of a minor who is clearly incapable of giving consent).

The Privacy Act does not give any indication about what age a child must be to be able to consent to the collection and use of their personal information. However the Privacy Commissioner takes the view that, when dealing with minors, consideration must be given to whether they have the mentally capacity to understand and give consent. Often students under the age of 18 will have this mental capacity.

The Privacy Commissioner takes the view that consent requires four elements:

1. It must be voluntarily given
    a. No coercion, duress or pressure;
    b. The individual is given a genuine opportunity to withhold consent;
    c. The individual must understand the alternatives; and
    d. The individual must understand the consequences.
2. The individual must be well informed
    a. Do they understand the implications of giving consent?
3. The consent must be current and specific
    a. It cannot be broad and must be specific;
    b. It must not have been withdrawn.
4. The individual must have the capacity to give the consent
    a. They must be capable of understand the issues and be able to form a view (they must have the maturity and understanding to do so);
    b. Schools can resort to a legal guardian if the individual lacks the capacity to give the consent, but even in such instances Schools should consider involving the individual in the process.

Schools may need to consider requiring older students applying for admission (for example, students who are in grade 10 through 12) to sign a document indicating either their consent to the collection of this information, or their consent for their parents or guardians to provide the School with their personal information. It would be unreasonable and impracticable to require the School to collect personal information directly from young students.

The other difficulty that Schools will face is where they collect sensitive information about a person from other individuals (such as fellow students). In such a circumstances, Schools will need to be cautious if

they decide to retain the sensitive information on file, without the consent of the particular individual concerned. This will be discussed further under the section "Unsolicited Personal Information".

APP 5: Notification of Collection

If possible, before, or as soon as practicable after collecting the personal information, a School must take reasonable steps to notify the individual of the matters referred to in APP 5.2.

These include:

- The School's contact details (APP 5.2(a));
- The fact that they have collected the information (if notice is being given after collection) and the circumstances of collection (such as date, time, method, place) (APP 5.2(b));
- Whether the collection is required or authorised by law (APP 5.2(c));
- The purpose of collection (this complements APP 3 – that the collection must be reasonably necessary for the functions or activities of the School) (APP 5.2(d));
- The consequences if the information is not collected (APP 5.2(e));
- The School's usual disclosures of information (APP 5.2(f));
    - The notice does not have to state that a particular disclosure is intended to or will occur. It must only state the "usual" disclosures made.
- Information about the School's Privacy Policy, and that it contains information about how the individual may access the personal information about the individual that is held by the School (APP 5.2(g)-(h));
- Whether the School is likely to disclose the information to overseas recipients[8] and the countries in which these recipients are located[9].[10]

To ensure that they have taken "reasonable steps", a school should develop procedures that are uniformly applied prior to collecting information. This could take the form of requiring that a standard collection notice for notifying individuals regarding the collection of personal information is sent out with the forms, or included in the body of the forms, that new enrolments must complete. If an individual is providing information via an online form, a School could require the individual to confirm that they have read the collection notice before the individual is able to provide their personal or sensitive information.

[8] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 104 (APP 5.2(i)).
[9] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 104 (APP 5.2(j)).
[10] Office of the Australian Information Commissioner, *Australian Privacy Principle 6 – use or disclosure of personal information* (September 2013) Office of the Australian Information Commissioner, 4 < http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/draft-australian-privacy-principles-guidelines/draft-app-guidelines>.

APP 3 and APP 5 may prove problematic for Schools who currently hold personal and sensitive information about students. As at 12 March 2014, Schools must have reviewed their policies and procedures to ensure that all information that they currently hold about students is in compliance with the requirements around the collection, and notification of collection under the APP's. If the way in which the School has previously implemented their procedures does not comply with APP 3 and APP 5, this information must either be re-collected in compliance with the APP's, or de-identified or destroyed.

The other difficulty with these requirements is where personal information (and particularly sensitive information) is collected on an ad-hoc basis. For example, teachers and counsellors may, from time to time, collect sensitive information from students (i.e. regarding health concerns, religious or political beliefs, sexual practices etc). Arguably, when collecting this information, the School (via the particular staff involved) may need to make the appropriate disclosures. This would need to be considered and addressed on a case by case basis.

2 STUDENT RECORDS

Once information about students has been collected and stored, these student records must be managed in a way that accords with the new APP's.

APP 1 – Open and transparent management of personal information

The overarching object of this APP is 'to ensure that APP entities manage personal information in an open and transparent way'. The School is held accountable for their personal information handling practices.[11]

As expressed in the APP Guidelines published by the Office of the Information Commissioner:

> *APP 1 lays down the first step in the information lifecycle – planning and explaining how information will be handled before it is collected. In effect, APP 1 reflects a principle of "privacy by design". Entities will be better placed to meet their privacy*

[11] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 2 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

> *obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices*[12].

APP 1 places three major obligations on Schools:

Obligation 1 - Procedures and compliance (APP 1.2)

Schools must take steps to implement new practices, procedures and systems that will:

- ensure that the School complies with the new APP's; and
- ensure that the School is able to deal with privacy inquiries and complaints from individuals[13].

APP 1.2, as well as being a general statement of obligation, requires Schools to take proactive steps to establish systems to ensure the School's compliance with the APP's[14]. We have already considered some if these obligations in the area of "collection" of personal information.

This obligation is measured by a 'reasonable steps' test. Whether a School has taken reasonable steps will depends on the circumstances of this School, including:

- The School's size, resources and business model;
- The nature of the personal information held. As the quantity, extent and sensitivity of the information held increases, Schools will be subject to stricter privacy standards;
- The adverse consequences for the individual if the School does not hold and manage their personal information in a way compliant with the APP's. As this information concerns minors, more thorough protections will have to be put in place surrounding this personal information;
- The practicability of developing and implementing these procedures and systems to comply with the APP's. The 'reasonable steps' test will be measured by the available options and cost to a

[12] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 2 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

[13] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 104 (APP 1.2(b)).

[14] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 3 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

School for implementing these measures. However, a School will not be exempt from this APP by arguing the excessive cost or inconvenience of doing so[15].

As a non-exhaustive example, taken from the APP Guidelines of the Office of the Australian Information Commissioner, Schools should implement practices and procedures addressing the following privacy matters:

- Procedures that regulate each step in the information lifecycle:
    - Collection
    - Use
    - Disclosure
    - Storage
    - Destruction
    - De-identification;
- Security systems for protecting access to the information and protecting these information records (including audit trails, backing up of computer systems, access control);
- Requirements to conduct an assessment of any new project where privacy information will be handled or disclosed;
- Procedures for identifying and reporting privacy breaches and receiving and responding to privacy related complaints and inquiries;
- Procedures giving individuals the option of not identifying themselves or using a pseudonym (as per APP 2) when dealing with the School;
- Overarching requirements to ensure APP compliance, such as the appointment of a privacy officer and the requirement of regular privacy reporting to the governance board of the School;
- Regular staff training;
- Periodic reviews of the School's ongoing compliance with its Privacy Policy and implemented requirements and procedures[16].

In establishing these procedures, Schools should keep a record of the steps that they have taken to comply with APP 1. This will demonstrate the School's openness and transparency of the handling of personal information from the initial steps.

---

[15] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 3 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

[16] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 3-4 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

Ultimately, Schools should organise for a detailed review by the School's legal representatives of the current systems in place governing the procedures to handle the personal and sensitive information currently in the possession of the School.

Obligation 2 – Developing an APP Privacy Policy (APP 1.3 and 1.4)

By 12 March 2014, Schools should have a Privacy Policy that is up-to-date and clearly expresses how Schools handle personal information. Many Schools will already have Privacy Policies. However, the APP's now stipulate with precision what must be included in the Policy.

The Privacy Policy must state the processes involved in collecting information, and what will happen to the information after it has been collected by the School. It does not need to state in detail the processes, procedures and compliance that is required by APP 1.2 (above), but it should give a brief overview of these processes.

There is no 'standard' Privacy Policy. It should be tailored towards the types of information handled by Schools. For example, it may categorize how different departments of the School will use the information that is collected about their students (such as the medical department, the administration department and the counselling department). If information between different classes of people will be handled differently or disclosed to a different audience, this should be explained. For Schools, this may include different disclosures regarding students with disabilities and learning difficulties.

Privacy Policies should be directed towards parties who are likely to read it. This will mainly be students, parents and guardians. It should be structured, clear, well set out, and avoid legal language.

This policy must include the matters set out in APP 1.4, which are:

- The types of personal information that the School holds (APP 1.4(a));
    - Personal information must be listed separately to sensitive information.
    - Example of person information holdings: Contact details, employment history, complaint details.
    - Example of sensitive information holdings: Mental health, disability, racial/ethnic origin, criminal convictions, religious affiliations, tax file numbers.[17]

[17] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 6 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

- How the School collect and holds personal information (APP 1.4(b));
- The purposes for which the School collects, holds, uses and discloses personal information (APP 1.4(c));
    - It should indicate the types of people/entities that are likely to access that personal information.
- How an individual can access the information about them that is held by the School, and how they can go about correcting that personal information if it is wrong (APP 1.4(d));
    - It should state:
        - That the individual has a legal right to request access to that information and to request that the information held about them be corrected (under APP 12 and 13).
        - The position description and contact details of the person to whom an individual may submit a request to access or correct the personal information held about them.
- How an individual can make a complaint against the School about an alleged breach of the APP's, and how the School will deal with such a complaint; (APP 1.4(e)):
    - The Policy should state the different stages of the complaint process:
        - A complaint should initially be made in writing to the School (*Privacy Act* s 40(1A)). The policy should include the contact details to make complaints to;
        - The School should be given a reasonable time of around 30 days to respond;
        - If the School does not adequately handle the complaint, then the complaint should be taken to an external source – which may be prescribed in the Policy to be an external dispute resolution scheme;
        - If the external dispute resolution scheme is not effective, the complaint may be taken to the OAIC.[18]
- Whether the School is likely to disclose the personal information to overseas recipients; and
- If the School is likely to disclose personal information to overseas recipients – the likely countries where such recipients are likely to be located. It should also state the types of information that are likely to be disclosed to entities in particular countries.

We suggest having your existing Privacy Policy formally reviewed by a legal practitioner to ensure compliance.

[18] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 7 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

Obligation 3 - Availability of APP Privacy Policy (APP 1.5)

It will also be required that Schools make their Privacy Policy available in an appropriate form, and free of charge[19]. This complies with the overall objective of APP 1 to make the information available in an open and transparent manner[20].

An appropriate way to provide the Privacy Policy in a way that complies with APP 1.5 is to make it accessible on the School's website.

Schools should, however, also take measures to make their Privacy Policy available to individuals who may not have internet access. This could include distributing printed handouts, inserting details about how to access the Privacy Policy included in all correspondence sent to School families or displaying it at the School's reception.

APP 6 – Use and disclosure of personal information

This APP regulates the use and disclosure of personal information that a School holds about an individual.

"Holds" is defined in section 6(1) of the Privacy Act. It means information that the School has possession or control over, and also extends to information that the School may not necessarily possess but nevertheless has the power to deal with. This could include personal information held on an external server that the School has the ability and power to access to retrieve the information.

"Use" is not defined and takes its usual meaning. It will include accessing or reading the information, searching records that contain the information, making a decision based on the information or passing the information from one part of the School to another part.

"Disclose" is also not defined and takes its usual meaning. Disclosure occurs where the information is made known outside of the School.

[19] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 104 (APP 1.5).

[20] Office of the Australian Information Commissioner, *Australian Privacy Principle 1 – Open and transparent management of personal information* (August 2013) Office of the Australian Information Commissioner, 8 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/current-privacy-consultations/Draft-APP-Guidelines-2013/Draft_APP_Guidelines_Chapter_1_APP_1.pdf>.

A School can only use and disclose personal information for the purpose for which it was collected (the "**primary purpose**"). It can be used for a purpose other than the primary purpose for which it was collected (the "**secondary purpose**") in certain circumstances. These circumstances are where:

- The individual consents to the use or disclosure (APP 6.1(a));
    - This can be express or implied consent. As already mentioned, the four main elements of consent are:
        - That to individual voluntarily provided the consent;
        - The individual was adequately informed;
        - The consent is current and specific; and
        - The individual has the capacity to communicate and give their consent.[21]
- The individual could reasonably expect the School to make that disclosure or use it for that secondary purpose and the secondary purpose is related to the primary purpose (or, for sensitive information, the secondary purpose is *directly* related to the primary purpose) (APP 6.2(a));
    - The School must only disclose the minimum amount of the information possible for the secondary purpose.
- A permitted general situation exists that allows the use or disclosure (APP 6.2(e)). These are:
    - Lessening or preventing a serious threat to life, health or safety;
    - Suspected unlawful action or serious misconduct;
    - Locating a missing person;
    - Establishing, exercising or defending a legal or equitable claim;
    - Where it is reasonably necessary for a confidential alternative dispute resolution process;
    - Necessary for a diplomatic or consular function/activity; and
    - Necessary for Defence Force activities outside Australia.[22]
- The use or disclosure is directed or authorised by law or by a court/Tribunal order (APP 6.2(b));
- A permitted health situation exists in relation to the secondary use disclosure (APP 6.2(d)). These are:
    - Conducting research;
    - Necessary to prevent a serious threat to life, health or safety; and
    - Disclosure to a responsible person for the individual.[23]
- The secondary use or disclosure is necessary for enforcement activities by an enforcement body. The necessity is at the discretion of the School (APP 6.2(e));

[21] Office of the Australian Information Commissioner, *Australian Privacy Principle 6 – use or disclosure of personal information* (September 2013) Office of the Australian Information Commissioner, 6 < http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/draft-australian-privacy-principles-guidelines/draft-app-guidelines>.
[22] *Privacy Act 1988* (Cth) s 16A.
[23] *Privacy Act 1988* (Cth) s 16B.

- If a School discloses personal information about an individual for this purpose, they must keep a written record of it and include the date, the information used or disclosed, the enforcement body, and the basis for the School's reasonable belief that the enforcement body needed it.

An important exception to note about this APP is that it does not apply to the disclosure of personal information for the direct marketing of the School.

3 SOCIAL MEDIA

Schools may become aware of personal or sensitive information about their students via social media. This may be via an alert by a concerned parent, inadvertently through word-of-mouth of other students in the School or by misdirected correspondence. These prominent social media sites will include Facebook, Instagram, Twitter and Tumblr.

APP 4 – Unsolicited Personal Information

As the School has not taken active steps to acquire this information and has not explicitly requested it from an external source, this kind of information will be classified as unsolicited personal information and will be governed by the rules of APP 4.

The Privacy Act defines "solicited" but does define "unsolicited". Therefore unsolicited information is all information that does not fit in the category as being actively solicited by the School. It will also include information provided to a School that is additional to the specific information that a School has solicited.

The main step that a School must take when they become aware of this information is to consider, as soon as reasonably possible after they receive the information, whether or not they could have solicited it under the rules of APP 3[24].

Information that could not have been collected in compliance with APP 3 must be destroyed or de-identified as soon as practicable[25]. Before it is destroyed, you must consider whether there is a law or legal order preventing it from being destroyed.

[24] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 104 (APP 4.1).

Information that could have been collected in compliance with APP 3 is to be treated in the same way as if it had been collected under that APP[26].

4 SURVEILLANCE

CCTV footage video surveillance that is recorded that identifies an individual is considered to be solicited personal information and is subject to the rules of APP 3.

5 OTHER CHANGES

The Australian Information Commissioner

The Australian Information Commissioner has the existing powers of being able to investigate complaints made by individuals that a School has breached the Privacy Act, make their own motion investigations, make determinations on complaints where conciliation has not been effective, to audit government agencies and some businesses, and deciding whether the disclosure of some personal information that would otherwise be prohibited should be allowed because disclosure is in the public interest[27].

The Australian Information Commissioner will gain additional powers, including:

- Being able to accept enforceable undertakings;
- Applying for penalties where there have been significant or repeated breaches of privacy of individuals;
- Assessing the privacy performance of businesses and government agencies[28].

Complaint handling for schools: External Dispute Resolution Schemes for Schools

[25] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) Schedule 1, Item 104 (APP 4.3).
[26] Office of the Australian Information Commissioner, *Australian Privacy Principle 4 – dealing with unsolicited personal information* (September 2013) Office of the Australian Information Commissioner, 4 < http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/draft-australian-privacy-principles-guidelines/draft-app-guidelines>.
[27] Australian Government, *Applying Privacy Law* (2013) Office of the Australian Information Commissioner <http://www.oaic.gov.au/privacy/privacy-act/applying-privacy-law>.
[28] Australian Government, *Privacy Law Reform* (2013) Office of the Australian Information Commissioner <http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform>.
130009 - 171318R3 - AJL

The Information Commissioner will gain the discretion of recognising External Dispute Resolution Schemes ("**EDR**") as an option to address complaints[29]. Each EDR Scheme will deal with a particular type or range of complaints. The Information Commissioner will recognise EDR schemes 'for a specified purpose', such as complaints relating to alleged breaches of specific sections of the Privacy Act[30]. A register of recognised EDR schemes, including the 'specified purpose' under which a scheme is recognised, will be maintained on the website of the Office of the Australian Information Commissioner. There is currently no register in existence.

The Information Commissioner may also choose not to investigate privacy complaints if they are satisfied that the complaint is being handled or addressed by an EDR Scheme[31], or would be more effectively dealt with by an EDR scheme[32]. The Act outlines what the Information Commissioner must consider in deciding to recognise EDR Schemes.

A School entity must 'implement practices, procedures and systems to address privacy-related enquiries and/or complaints from individuals (APP 1.2)[33]. This will include becoming a 'member' of a recognised EDR scheme as a way to resolve complaints.

A complaint by an individual will generally be addressed by a three-stage process:

- An individual complains to the APP entity;
- If an individual is not satisfied with the response offered by the APP entity, the individual can complain to a recognised EDR scheme of which the APP entity is a member;
- If the APP entity is not a member of an EDR scheme, or the individual is not satisfied with the outcome of the ADR scheme, the individual may make a complaint to the Information Commissioner under section 36 of the Privacy Act[34].

---

[29] *Privacy Act 1988* (Cth) s 35A.

[30] Office of the Australian Information Commissioner, *Guidelines for recognising external dispute resolution schemes under s 35A of the Privacy Act 1988* (September 2013) Office of the Australian Information Commissioner, 5 <http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/guidelines-for-recognising-external-dispute-resolution-schemes>.

[31] *Privacy Act 1988* (Cth) s 41(1)(dc).

[32] *Privacy Act 1988* (Cth) s 41(1)(dd).

[33] Office of the Australian Information Commissioner, *Guidelines for recognising external dispute resolution schemes under s 35A of the Privacy Act 1988* (September 2013) Office of the Australian Information Commissioner, 4 <http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/guidelines-for-recognising-external-dispute-resolution-schemes>.

[34] E Office of the Australian Information Commissioner, *Guidelines for recognising external dispute resolution schemes under s 35A of the Privacy Act 1988* (September 2013) Office of the Australian Information Commissioner, 4 <http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/guidelines-for-recognising-external-dispute-resolution-schemes>.

130009 - 171318R3 - AJL

APP 8 – Cross-Border Disclosure of Personal Information

There has been a recent shift to cloud computing, that is, the virtual storage of information by a storage provider. Often these providers are located overseas, resulting in the disclosure of personal information over international borders.

APP 8 imposes an obligation on Schools, if they use cloud computing, to take reasonable steps to ensure that the overseas provider does not breach the APP's. This imposes an additional obligation upon them in a similar way to the other privacy principles.

Schools will not have to comply with this requirement if:

- The recipient of the information is subject to a similar structure or scheme that has the effect of protecting the information a similar way that the APP's would; or
- The recipient of the information informs the individual that if they provide consent to the disclosure, that APP will not apply to the disclosure and the individual then consents to the disclosure.

If you need to review your policies and procedures in light of the upcoming changes to privacy law, our team of legal professionals can assist you.