Briefing Paper

The Privacy Laws & Australian Privacy Principles

Who should read this briefing paper?

- Governors - Principals - Executives - Business Managers -

The information in this briefing paper is current as at 14 January 2016. Please visit www.complispace.com.au to ensure that you have the most up-to-date version of this briefing paper.

Sydney Level 4, 179 Elizabeth St, Sydney NSW 2000 T: +61 2 9299 6105 F: +612 9299 2805

Perth Level 1, 28 Kintail Road, Applecross, WA 6153 T: 08 9460 5200

Melbourne Suite 203, 35 Whitehorse Road, Balwyn VIC 3103 T: 1300 132 090

contactus@complispace.com.au www.complispace.com.au CompliSpace Pty Ltd ABN 67 151 135 072

Prepared by:

complispace
make it work

Table of Contents

1. Executive Summary

- ✓ On 12 March 2014 **substantial changes** to Australia's existing **Privacy laws** commenced, which affect how Non-Government Schools ("Schools") handle personal information. These new laws introduced **13 Australian Privacy Principles (APPs)** with which Schools must comply**.**

- ✓ The laws apply to all Schools, unless they have annual revenues of less than $3 million and they do not provide a health service. The new laws do not apply to State and Territory government schools (which are subject to local privacy laws).

- ✓ The APPs introduced new obligations which include stricter rules on sending personal information **overseas**, **complaints** handling procedures, the use of personal details for **direct marketing**, the **security** of personal information and the treatment of **unsolicited personal information**.

- ✓ A central feature of the new laws is that Schools must have **procedures, practices and systems**, integrated within their organisational governance framework, to ensure compliance with each of the 13 APPs (**Compliance Program**) and to manage privacy queries and complaints (**Complaints Handling Program**). This requirement is referred to as "**Privacy by Design**".

- ✓ The new laws require Schools to have a documented **Privacy Program** in place which sets out clearly the **why** (why do you need to comply); the **what** (what do you have to do); the **how** (how you comply with each of the 13 APPs); the **who** (who is responsible for particular parts of privacy compliance); and the **when** (when and at what frequency do things need to be done).

- ✓ The new laws also require Schools to publish a clear and specifically worded disclosure statement (referred to as a **Privacy Policy**) that spells out the types of personal information they collect and hold, how they collect and store the information, and the purposes for which they use and disclose personal information.

- ✓ Also central to compliance, Schools must ensure that other systems and procedures are in place, such as those governing **ICT** and **physical security,** as well as human resources policies covering **workplace surveillance**, **email and internet monitoring**, **social media usage,** and of course **staff training**.

- ✓ The **Privacy Commissioner** has **expanded powers** under the new laws, including the ability to conduct Performance Assessments of Schools to determine whether they are handling personal information in accordance with the 13 APPs.

- ✓ The Privacy Commissioner is able to seek enforceable undertakings, or apply through the courts for civil **penalties** of up to **$1.8 million** for companies or **$360,000** for individuals for breaches of the Privacy Act.

- ✓ To comply with these changes, Schools should conduct a **Personal Information Management Audit**, document their Privacy Program and ensure that they publish a new Privacy Policy on their public website.

- ✓ Failure to establish and effectively implement procedures, practices and systems to comply with the new Privacy laws presents a significant risk for a School. **Reputational damage** is an obvious consequence, in the event that a School community discovers that a School's board and executive were either unaware of the School's privacy obligations, or simply chose to ignore them.

- ✓ **Ten Steps to Ensuring Privacy Compliance** are set out at the end of this briefing paper.

2. Enterprise Risk Management

The 2014 amendments to the Privacy Act 1988 (Cth) introduced 13 new Australian Privacy Principles (APPs) with which Non-Government Schools must comply.

Unlike the previous privacy regime, which was regarded as being relatively ineffective, the current laws require:

- ✓ Schools to implement internal practices, procedures and systems, integrated within their organisational governance framework, that ensure that they comply with each of the 13 APPs and are able to deal with enquiries or complaints from individuals about their compliance. Simply publishing a privacy statement on your public website is not enough;
- ✓ Additional controls on how personal information can be used for secondary purposes such as direct marketing;
- ✓ Obligations for Schools that disclose personal information to overseas recipients (think "cloud providers", overseas excursions and student exchange programs); and
- ✓ Obligations for Schools to secure and protect personal information (think both IT security and physical security) and to provide access to, and ensure correction of, personal information.

The current laws also provide the Federal Privacy Commissioner "with teeth" through the provision of new investigatory and enforcement powers, and the ability to hand out penalties of up to $1.8M for entities and $360,000 for individuals who breach the Privacy Act.

3. Why is Complying with the Privacy Laws Important?

A survey by the Office of the Australian Information Commissioner, found that 90% of people are concerned about cross-border disclosure of their personal information and 60% had decided not to deal with an organisation because of privacy concerns (up from 40% in 2007).

Given that many Schools hold the personal information (including sensitive information) of thousands of individuals (students, parents, prospective parents, staff, alumni, volunteers), by sheer weight of numbers, it is likely to be a matter of "when" not "if" a privacy breach occurs. How your School responds to a privacy breach, and how it will be judged in the eyes of your School community, will ultimately be determined by the work that your School has undertaken to ensure compliance with the new Privacy laws.

Failure to understand your obligations, and failure to take appropriate steps to ensure compliance with the Privacy laws, will undoubtedly lead to reputational damage.

"If an organisation mishandles the personal information of its clients or customers, it risks the serious financial consequences associated with remediation, loss of trust and considerable harm to the organisation's reputation, loss of customers and even serious impact on the organisation's capacity to perform its core functions or activities …The business case is simply that good privacy practice is good business practice"

Timothy Pilgrim, Privacy Commissioner

Presentation to Privacy Awareness Week 2013 Business Breakfast, 29 April 2013

4. What is Personal Information?

When it comes down to it, Privacy laws are all about how you handle the "Personal Information" you collect from individuals who deal with your School. These individuals may be students, parents, prospective parents, staff, prospective staff, volunteers, alumni, suppliers … the list goes on.

"Personal Information" is the general term that is used to describe information or an opinion about an identified individual, or an individual who is reasonably identifiable.

"Personal Information" includes "Sensitive Information" and "Health Information". "Health information" is a subset of "Sensitive Information".

- ✓ **Personal Information** includes such information as a person's name, address, financial information, marital status or billing details.

- ✓ **Sensitive Information** includes information with respect to an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record as well as health and genetic information.

- ✓ **Health Information** includes any information collected about an individual's health or disability and any information collected in relation to a health service that is provided. It includes such things as notes of symptoms, diagnosis or treatments, doctor's reports, appointment times and prescriptions.

The Privacy laws regulate personal information that is contained in a **"record"** (e.g. written down, on a database, in a photograph or video etc.). If personal information is not recorded it is not regulated by the Privacy Act.

5. Risk & Compliance Reporting

The Privacy Act does not differentiate between adults and children, and does not specify an age after which individuals can make their own decisions with respect to their personal information.

This raises some interesting issues for Schools concerning the question of whether consents should be obtained from a student's parents or directly from students themselves. It also potentially raises issues with respect to disclosure of personal information (particularly sensitive information).

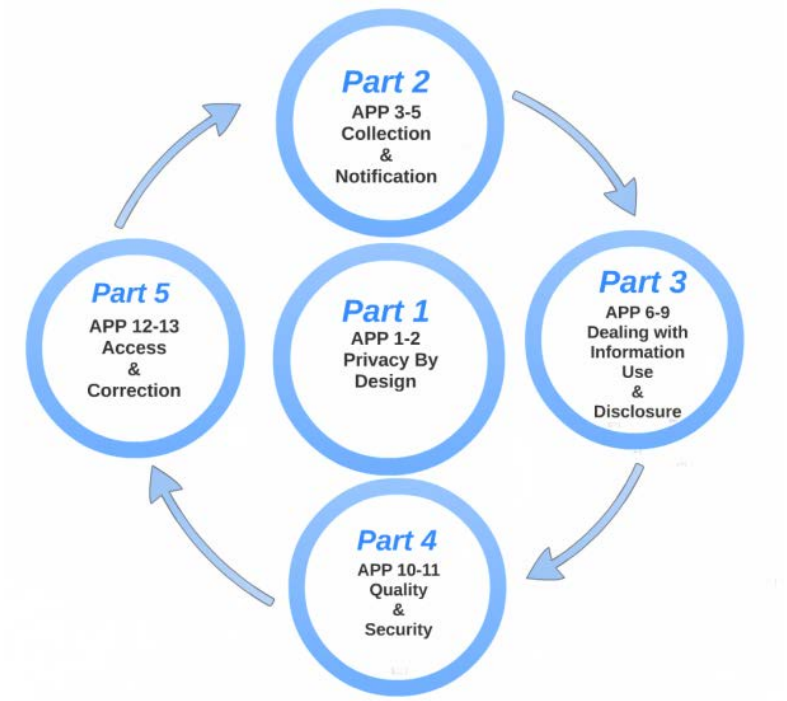
Having regard to the fact that parents generally have the right to make decisions for their children until they reach 18 years of age, and the fact that Schools have a direct contractual relationship with a student's parents, it is expected that Schools will generally take the view that notifications provided to parents will act as notifications to students and consents received from parents will act as consents given by students.

That said, Schools need to be cognisant of the fact that children do have rights under the Privacy Act and that, in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. Situations where a student requests that personal information (particularly sensitive information) not be disclosed to parents should be dealt with on a case by case basis.

6. Risk & Compliance Reporting

The 13 APPs are structured within a Privacy Information Life Cycle as illustrated in Figure 1.

Figure 1: Privacy Information Life Cycle



Part 1 – Privacy by Design	
APP 1: Open and transparent management of personal information.	Schools are required to implement practices, procedures and systems that ensure they comply with each of the 13 APPs and are able to deal with enquiries or complaints from individuals related to privacy. This requirement reflects a principle of "Privacy by Design". APP 1 also requires a School to have a clearly expressed, up-to-date and freely available Privacy Policy that sets out how it manages the personal information it collects.
APP 2: Anonymity and pseudonymity	Individuals have the option of not identifying themselves, or of using a pseudonym, when dealing with a School covered by the APPs.
Part 2 - Collection & Notification	
APP 3: Collection of solicited personal information	A School must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of its functions or activities. Subject to a number of exceptions, Schools can only collect "sensitive information" if the individual consents to the collection.
APP 4: Dealing with unsolicited information	If a School receives personal information that it did not solicit, it must decide whether or not it could have collected the information under APP 3. If not, the School must, as soon as practical, destroy the information or ensure it is de-identified.
APP 5: Notification of the collection of personal information	At or before the time of collection (or as soon as practical thereafter) Schools must take reasonable steps to notify an individual about, or ensure an individual is aware of, certain prescribed information concerning the purpose and circumstances of the collection of their personal information.

Part 3 – Dealing with Personal Information Use & Disclosure	
APP 6: Use or disclosure of personal information	A School can only use or disclose personal information for the primary purpose for which it was collected, for a secondary purpose where the individual has consented, where disclosure is required by law, where a Permitted Health Situation or a Permitted General Situation exist, or if the individual would reasonably expect the use or disclosure, and the secondary purpose is related to the primary purpose (or "directly" related in the case of sensitive information).
APP 7: Direct marketing	A School must not use or disclose personal information it has collected from an individual for the purpose of direct marketing unless it has the individual's consent, or if it is impractical to obtain consent for each direct marketing communication, the School provides the individual with the ability to "opt out" of receiving future direct marketing communications. Sensitive information cannot be used for direct marketing purposes without an individual's consent.
APP 8: Cross-border disclosure of personal information	Where a School discloses personal information to an overseas recipient (such as a cloud service provider), it must take reasonable steps to ensure that the overseas recipient does not breach the APPs. A School will be legally accountable if the overseas recipient mishandles the personal information, unless the School has the individual's consent to the overseas disclosure, or the School satisfies itself that the overseas recipient is subject to the laws of a country, or a binding scheme, that it reasonably believes to be substantially similar to the protections provided by the 13 APPs and the individual can access a mechanism to enforce those protections.
APP 9: Adoption of government-related identifiers	A School must not adopt a government-related identifier as its own identifier of an individual.
Part 4 – Quality and Security	
APP 10: Quality of personal information	A School must ensure that the personal information it collects, uses or discloses is accurate, up-to-date, complete and relevant.
APP 11: Security of personal information	A School must take reasonable steps to secure personal information and protect it from misuse, interference, loss, unauthorised access, modification or disclosure. Where a School no longer needs the personal information it must destroy or de-identify it.
Part 5 – Access and Correction	
APP 12: Access to personal information	Where a School holds the personal information of an individual, with limited exceptions, it must upon request by that individual, provide the individual with access to the information.
APP 13: Correction of personal information	A School must take reasonable steps to correct any personal information that is inaccurate, out of date, incomplete, irrelevant or misleading. If the School has disclosed information to another organisation, it must take reasonable steps to notify that organisation of any corrections where the individual has requested the School to do so.

Privacy by Design

One of the most significant changes under the 2014 amendments to the Privacy Act was the requirement for Schools to adopt a "Privacy by Design" approach which involves developing internal practices, procedures and systems that ensure you comply with the 13 Australian Privacy Principles (APPs). To satisfy this obligation a School should:

- ✓ Document a **Privacy Program** that sets out the why (why do you need to comply); the what (what do you have to do); the how (how are you going to comply with each of the 13 APPs); the who (who is responsible for particular parts of privacy compliance); and the when (when and at what frequency do things need to be done).

- ✓ Undertake an audit of how it currently handles personal information in order to properly understand its current systems and to establish whether it has any compliance gaps (**Personal Information Management Audit**).

- ✓ Publish a **Privacy Policy**, which is essentially a disclosure document that should be published on its public website, describing how it manages the personal information it holds.

- ✓ Ensure that a **Privacy Collection Notice** is incorporated into the forms it uses to collect personal information.

Privacy Does Not Operate in a Vacuum

Compliance with Privacy laws requires a lot more than simply publishing a "Privacy Policy" on your School's public website, or putting a Privacy Collection Notice on a form. Privacy laws require a School to incorporate privacy compliance into its existing governance infrastructure and into its day-to-day operations. In this regard a School should:

- ✓ Incorporate key privacy obligations into its **Compliance Program** so that they can be effectively monitored, and assurance with respect to compliance can be provided to a School's executive team and its board.

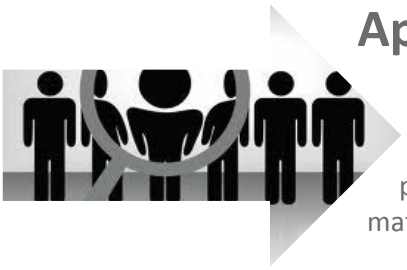
- ✓ Ensure it has a functional **Complaints Handling / Incident Management Program** through which it is able to capture and manage privacy enquires or complaints.

- ✓ Use its **Risk Management Program** (if a School has one) to identify key privacy related risks, assess them and effectively control them.

- ✓ Establish and effectively implement **organisational policies and procedures** that are designed to ensure privacy compliance at an operational level. Typical policies would include those covering matters such as **Workplace Surveillance**, the use of **Personal Devices**, **Social Media**, **Security** of Buildings and Grounds, **ICT Security**, **Email and Internet Usage** and **Management of Confidential Waste**.

- ✓ Ensure that all **staff receive training** with respect to their privacy obligations and the School's expectations with respect to the management of personal information.

Appointment of a Privacy Officer



A School with 1500 students will have approximately 3000 parents, potentially 3000 prospective parents and 10,000 alumni, meaning that it may hold the personal records of 15 -20,000 individuals. Sheer volume means that it is not a matter of "if" but "when" a privacy incident, complaint or breach occurs.

In these circumstances it is incumbent on a School's executive to ensure that at least one person has a good understanding of the Privacy laws and takes the lead in ensuring that your School is compliant. Appointment of a Privacy Officer (it is not envisaged that this would be a dedicated position) will ensure that someone in the School is primarily responsible for integrating privacy obligations into existing practices, procedures and systems and promoting a culture where the personal information of individuals is protected in accordance with your obligations under the Privacy Act.

Tailoring Your Privacy Policy

A School's **Privacy Policy** is the primary means through which it complies with its obligation under **APP 5** (**Notification of Collection of Personal Information)** to take reasonable steps to disclose certain information specified in the Privacy Act to individuals, at the time of collection.

A Privacy Policy also plays a critical role in clearly stating the "**primary purpose**" for which information is collected and establishing "**reasonable expectations**" as to how your School may use, or disclose, personal information for a related secondary purpose (or for a "directly" related secondary purpose in the case of sensitive information) under **APP 6 (Use or Disclosure of Personal Information)**.

The importance of clearly establishing your "primary purposes" and setting "reasonable expectations" is that you will effectively minimise your need to obtain specific consents. This will in turn reduce the resources that your School will need to commit to the administration of such consents.

Direct Marketing Opt Outs

The Privacy laws contain specific rules on how Schools can use or disclose personal information for direct marketing purposes. These requirements are outlined in APP 7.

Direct marketing can be a catalogue or brochure addressed to an individual by name, an advertisement on a social media site that an individual is logged into, or correspondence sent to a former student of a School promoting a School-related event or activity.

Under APP 7, if it is impracticable to obtain consent with respect to each direct marketing communication (which it usually is), Schools can still use personal information for direct marketing purposes if the School provides individuals with a simple, prominent statement on its website and in each of its communications, providing a means to "opt-out" of receiving further direct marketing communications.

Cross-border disclosure of personal information

The Privacy laws contain a requirement for a School to take reasonable steps to ensure an overseas recipient they disclose personal information to does not breach Australian Privacy law. These requirements are contained in APP 8 (Cross-border disclosure of personal information).

Cross-border disclosure of personal information can include the sending of an email to an overseas recipient containing personal information, the storage of a document containing personal information on a foreign cloud-based computing storage service, or the backing up of a contact list on a mobile device – such as an iPad or iPhone – to the cloud.

Schools should conduct a Personal Information Management Audit to identify all the foreign-based recipients of personal information they manage. They may not be obvious at first sight.

There are some exemptions to organisations being liable for any breaches of Australian Privacy laws by a foreign recipient.
These include:

- ✓ Where the overseas recipient is subject to a law, or binding scheme, that affords substantially similar protections to those in the APPs and the individual can access an enforcement mechanism to enforce those protections.

- ✓ An organisation gains consent from an individual that their personal information will be disclosed to an overseas recipient (and will not be protected by Australian Privacy law) after providing express notification.

Integrity and Security of personal information

The Privacy laws place stronger obligations on Schools to ensure they properly manage and secure the personal information that they collect.

APP 10 (Quality of personal information) requires Schools to take reasonable steps to ensure the personal information that they hold is accurate, up-to-date, complete and relevant. To fulfill this requirement, Schools must have practices, procedures and systems in place to ensure that they capture changes in personal information and update them in all of their records. This would include establishing procedures to manage things such as email bounce backs, returned mail and communications from individuals correcting their personal information.

APP 11 (Security of personal information) creates an obligation for Schools to protect personal information from "interference". This will require Schools to think more laterally and take reasonable steps to protect themselves against activities such as computer "hacking" attacks and the protection of personal information that may be stored on personal devices such as mobile phones.

Handling Enquiries and Complaints

Whilst all Schools are required to have complaints handling systems in place as part of their registration requirements, it is well known that this is a governance discipline with respect to which many Schools struggle.

A central compliance obligation under the APPs is that a School must advise individuals in their Privacy Policy of how they can complain and will also need to have practices, systems and procedures in place to manage complaints as they arise.

It is recommended that all Schools carefully review their complaints handling systems in line with the Privacy laws published on 12 March 2014. Schools need to train their staff so that they understand the School's privacy obligations and are in a position to respond appropriately to privacy enquiries and complaints.

Record Keeping

Secure and organised record keeping procedures are essential in order to comply with the Privacy laws. The term 'record' is broad and can encompass a variety of forms of recording information, including in hard and soft copy, writing, photographs, video/films and audio.

As Schools are required to destroy or de-identify personal information when it is no longer needed, there must be a clear policy as to what information is 'needed'. This term is not defined by the APPs but Schools should look to the individual authorities of their State and Territory for guidance and develop a system for ensuring records are managed correctly.

Another factor that Schools should consider is the possibility of future legal proceedings. Schools may be called upon to produce evidence relating to a student or a member of staff at some point in the distant future and, from a risk and reputational management perspective, it is important to have in place effective long-term document storage resources.

If Schools do have a policy of retaining records indefinitely, there must be a process to determine whether the records in question are personal records. Schools can then evaluate, based on their obligations under the Privacy laws, whether they can lawfully retain these records or whether they must be destroyed (see APP 11).

Credit Reporting

In April 2014 the Privacy (Credit Reporting) Code was introduced. The Code supplements the credit reporting provisions in the Privacy Act and it binds credit providers and credit reporting bodies. In some cases, schools may be considered to be credit providers under the Privacy Act. As a result, they may possess credit information that is also personal information which must be dealt with in accordance with the APPs and the Code.

Schools that are credit providers are required to implement policies and procedures in accordance with the credit reporting provisions of the Privacy Act, in addition to complying with their obligations under the APPs to ensure that they manage credit information in an open and transparent way.

8. Privacy Compliance Checklist

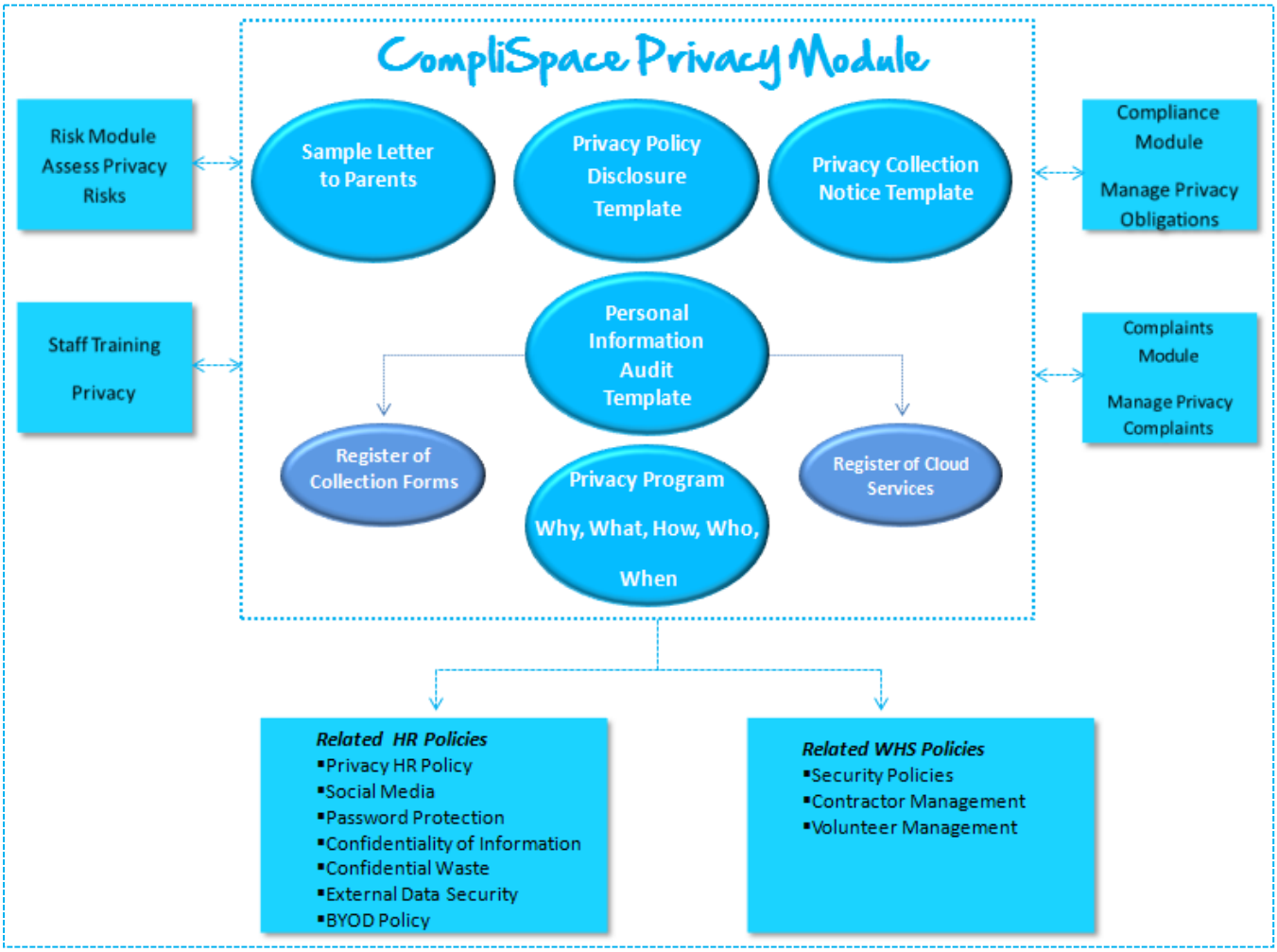
Here's a list of things to do in order to ensure that your School is compliant with its privacy obligations.

Task	Completed
Document Your School's Privacy Program (why, what, how, who, when)	☐
Appoint a Privacy Officer	☐
Complete your Personal Information Management Audit	☐
Review your Personal Information management and security practices, systems and procedures and close any gaps	☐
Ensure all Information Collection Forms include a Privacy Collection Notice	☐
Ensure all direct marketing communications set out clear "opt out" provisions	☐
Ensure that your complaints and incident management systems are working	☐
Tailor your Privacy Policy to ensure that it fits your School's approach to managing your privacy obligations	☐
Train your staff on privacy issues	☐
Publish your Privacy Policy on your public website	☐
Notify parents (and other key stakeholders) that your new Privacy Policy has been published	☐
Establish practices, systems and procedures to ensure your School's ongoing compliance with your privacy obligations through a Compliance Program	☐
Establish practices, systems and procedures to ensure that your Privacy Program is being effectively monitored and regularly reviewed.	☐

9. How CompliSpace Can Help

CompliSpace combines specialist governance, risk and compliance consulting services with practical, technology-enabled solutions.

As illustrated below our privacy module is presented within an integrated governance framework that enables a school to manage personal information effectively and meet its privacy obligations on an ongoing basis.



If you are looking to update your existing Privacy Program contact us on:

T: 1300 132 090
E: contactus@complispace.com.au
W: http://www.complispace.com.au

Disclaimer
This briefing paper is a guide to keep readers updated with the latest information. It is not intended as legal advice or as advice that should be relied on by readers. The information contained in this briefing paper may have been updated since its posting, or it may not apply in all circumstances. If you require specific advice, please contact us on 1300 132 090 and we will be happy to assist.

