WHITE PAPER

Schools, Privacy and the Australian Privacy Principles

For Board members, Principals, Executives, Business Managers

CompliSpace Pty Ltd | 1300 132 090
www.complispace.com.au
www.schoolgovernance.net.au

ACT | NSW | NT | QLD | SA | TAS | VIC | WA

Published by:

complispace SchoolGovernance

Table of Contents

1. Executive Summary

- ✓ In 2014 the federal government amended the Privacy Act 1988 (Cth) (**Privacy Act**) by introducing the **13 Australian Privacy Principles (APPs)** which specify how organisations must handle personal information.

- ✓ The 13 APPs apply to all non-government schools that provide a health service or have an annual turnover of more than $3 million.

- ✓ A central requirement of the APPs is that schools must have **procedures, practices and systems**, integrated within their organisational governance framework, to ensure compliance with each of the 13 APPs. This requirement is referred to as "**Privacy by Design**" and should be documented in your school's **Privacy Program**.

- ✓ To identify any gaps in compliance with the APPs, a school should conduct a **Personal Information Management Audit to** identify all of the personal information it collects and holds, how it uses and discloses it, how it ensures that it is accurate and current, and how it stores and disposes of it.

- ✓ Schools are required to publish a clear and specifically-worded disclosure statement (**Privacy Policy**) that spells out the types of personal information they collect and hold, how they collect and store the personal information, the purposes for which they use and disclose personal information, and how to contact the school in relation to the access or amendment of personal information, or queries or complaints about the way the school manages personal information. The Privacy Policy should be on a school's website or equivalent.

- ✓ Schools must ensure they have in place other systems and procedures in addition to the Privacy Policy, such as those governing **ICT** and **physical security,** and human resources policies covering **workplace surveillance**, **email and internet monitoring**, **social media usage, and confidentiality and privacy requirements in conditions of employment or codes of conduct**.

- ✓ When collecting personal information, schools are required to issue tailored collection notices to ensure that an individual is aware of the specific purpose for which their personal information is being collected.

- ✓ Schools must publish procedures to enable individuals to request access to, amend, query and complain about their personal information.

- ✓ Schools must have procedures in place to respond to data breaches relating to personal information, including procedures for notifying affected individuals and the Office of the Australian Information Commissioner (OAIC).

- ✓ School staff must receive training and regular refreshers to ensure that they understand their roles and responsibilities in relation to handling personal information and responding to data breaches.

- ✓ Failure to comply with privacy laws presents significant risks for a school, including reputational damage as well as civil penalties of up to $2.1 million for companies for breaches of the Privacy Act.

- ✓ **13 Steps to Ensuring Privacy Compliance** are set out at the end of this White Paper.

2. Why is Privacy Important?

In an age where individuals expose their innermost thoughts, feelings and images on social media to a potential audience around the world, it may seem counterintuitive that increased attention is being paid to the privacy of personal information and higher penalties are being imposed to protect it.

Whatever the drivers, it is hard to dispute that misuse or unauthorised disclosure of personal information can cause great harm to individuals, whether it be financial, physical, social, psychological or reputational. From the initial changes in 2014, when the Privacy Act was amended to apply the 13 APPs to the private sector with real penalties for breaches, to the most recent changes which require individuals to be notified as soon as practicable if a data breach is likely to cause serious harm, the message is very clear that maintaining the privacy of personal information is important.

3. Does the Privacy Act Apply to Your School?

The Privacy Act applies to non-government schools where:

- they have an annual turnover of more than $3 million
- they're connected to a larger organisation (with an annual turnover of $3 million)
- they supply a health service and hold health information (even though this isn't their primary activity).

A school is considered by the privacy regulator to be supplying a "health service" where it keeps records of a child's medical condition or general health, and provides other health related activities such as first aid and administration of medication. Given the breadth of the interpretation of "health service", it is extremely likely that all schools should consider themselves covered by the Privacy Act. If a school is not sure whether the Privacy Act applies to them, it is strongly recommended that in the interests of risk management and good confidentiality practice, they seek to comply.

4. Privacy by Design

The Privacy Act introduced the concept of "privacy by design" – which requires an organisation to proactively plan privacy protections. This involves reviewing each element of the "privacy information life cycle". These elements are: collection, use and disclosure, quality of information, security of information, individuals' access to information, corrections, complaints and the destruction of information that is no longer required. By reviewing all these elements, a school can identify areas of non-compliance or risks of non-compliance in its activities, and take appropriate measures.

5. What is Personal Information?

The Privacy Act is all about protecting "personal information". For schools to maintain their normal operations and discharge their duty of care towards students and workers, they need to collect personal information from parents/guardians, students, job applicants, contractors, and volunteers. Schools usually collect this information at the beginning of the relationship and add to it over time.

The Act defines "personal information" as:

"Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a. whether the information or opinion is true or not; and

b. whether the information or opinion is recorded in a material form or not."

Obvious examples of personal information about an identified individual include an individual's name, address, financial and credit details, image, health information, religious beliefs, sexual orientation, racial or ethnic origins, a past employment record (but not relating to a current employee), and Medicare or Centrelink details.

Sadly, working out what is meant by "information or an opinion about … an individual who is reasonably identifiable" is much less straightforward. Whether the individual can reasonably be identified from some information may depend on the particular circumstances and context, and may involve relating different pieces of information together to identify a person.

The **OAIC** warns of the "dynamic nature of information", so that while information may not be identifying when it is first collected it may become so at a later point. This sounds confusing, if not alarming, but it can be made clearer with an example. Imagine that someone complains about an event anonymously, but reveals some personal information about themselves during the process, for instance, that they are male. At this stage the information is not identifying, but if the school subsequently discovers that there was only one male present during the event, the information becomes identifying.

The other matter to note is that the individual need not be "identifiable" to everyone, so while a blurry image in a school publication would not be identifiable to the general public, members of the school community would be able to identify the person.

And the final confusing point to note is that personal information need not be recorded in a "material form" which means that the definition includes information shared orally, as well as including the more obvious hard copy documents, electronic data, images, signs, video and voice recordings. While it is possible to have a data breach under the Privacy Act where someone mistakenly or deliberately leaks personal information orally, many of the APPs only apply in relation to a "record" which the entity "holds".

Personal information is sub-divided in the Privacy Act and assigned different levels of protection based on its perceived level of confidentiality. Health records, and other "sensitive personal information" require additional consent and limits on use for purposes other than the notified primary purpose. "Sensitive personal information" includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record. Credit information where the holder is a credit reporting agency has its own substantial set of rules in the Privacy Act.

Not all personal information relating to an identified individual is covered by the Privacy Act - information relating to a deceased person and information held in specified categories of public record, are excluded. There is also an explicit exemption of employee records collected in the course of normal employment operations.

The OAIC guide ***What is Personal Information*** provides more information on the conundrums relating to the definition of "personal information".

6. The Role of the Privacy Policy

A Privacy Policy is the overarching document that explains the type of personal information the school collects, what it will be used for and which third parties may be accessing the information. It also sets out how an individual whose personal information has been collected can access that information, amend that information, or complain about how the school handles that information. APP 1 sets out the specific elements which must be addressed in the school's Privacy Policy.

As APP 1 also covers "open and transparent management of personal information", it requires a school's Privacy Policy to be published, easily accessible and available in a form that an individual whose information is being collected can understand. Basically, it should be on a school's website and all communication where personal information is collected should include a reference to the Privacy Policy.

The Privacy Policy works in conjunction with "collection notices". Unlike the Privacy Policy, which covers collection and use of information generally, collection notices are attached at information collection points and relate to the specific purpose and use of that particular information.

The Privacy Policy is the foundation of a school's compliance with the Privacy Act, but it is worthless unless it reflects the actual workings of the school in managing personal information. A Privacy Policy must be underpinned by detailed procedures which provide guidance to staff at all levels on how to manage personal information.

7. Collecting Personal Information

The key to complying with the Privacy Act when collecting personal information is to:

- only collect information that is reasonably necessary for, or directly related to, one or more of the school's functions or activities, and
- ensure the individual whose information is being collected is made aware of what the purposes of collection are at the time of collection.

In certain circumstances consent may be required from the individual before their information can be collected or used. Consent is often required when dealing with "sensitive information", including health information as well as information or opinion relating to an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, some of which is required by law to be collected by schools.

A key compliance requirement for schools when collecting information is ensuring that, where practicable, the individual is given a "collection notice". This sets out the purpose for which the information is being collected and how it will be used and disclosed. APP 5 has very specific requirements on what must be included in the notice, and the notice must reflect the specific information, rather than a generic notice to go with any information collection. For example, a collection notice when collecting student health information before going on an overseas tour would include what the information will be used for, who outside the school may be accessing it, and the protections afforded the information in the countries where it would be made available on the tour.

8. Using and Disclosing Personal Information

Broadly speaking, the Privacy Act's provisions on "open and transparent management of personal information" aim to ensure that individuals understand what will be done with the information they provide to an organisation so that they can then choose whether to provide it or not. A collection notice should accompany any request for information and must set out the purposes for which the information will be used. Once again, this is not completely straightforward because the Act describes "primary" and "secondary" purposes.

According to the OAIC guidance, the "primary purpose" is the specific function or activity for which the school collects the personal information. The "secondary purpose" is "any purpose other than the primary purpose". APP 6 provides that the school can only use or disclose personal information for a purpose for which it was collected (the "primary purpose"), or for a secondary purpose if an exception applies. The exceptions include where:

- the individual has explicitly consented for the information to be used for a secondary purpose
- the school is required by law or a court/tribunal order, to disclose this information
- the school is required by law enforcement to disclose the information
- the school has reason to suspect that unlawful activity or misconduct of a serious nature that relates to the school's functions or activities has been, is being, or may be engaged in, and it is necessary to use or disclose the information to take appropriate action
- using or disclosing the information would lessen or prevent a serious threat to life, health or safety of an individual or public health or safety
- the information is needed to locate a person who has been reported as missing.

These are the simple exceptions. There is a trickier one. Under APP 6 a school may disclose personal information for a secondary purpose if there is:

- implied consent: where it is reasonable for the school to believe that the individual would reasonably expect that the information would be used for that secondary purpose.

A straightforward example of implied consent is where a parent gives consent for their child to participate in an inter-school athletics competition. In this scenario it would be reasonable for the school to believe that the parent would expect that their child's name and relevant details would be passed to the competition organisers.

The situation is less straightforward when it comes to "sensitive information" and secondary purposes. Under the Privacy Act, sensitive information includes health information as well as personal information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record. A school may only use sensitive personal information for a secondary purpose if they have consent or the secondary purpose is *directly related* to the primary purpose of collection. The **OAIC** explains "directly related" purpose to mean "one which is closely associated with the primary purpose even if it is not strictly necessary to achieve that primary purpose." While this is not terribly helpful, the gist is that if a school is considering using sensitive information for a secondary purpose it should carefully consider whether the individual really would expect that the sensitive personal information would be used for that purpose and would not object.

An area of frequent concern for schools is whether student information can be published on external websites. For example, can the sporting or academic achievements of identified individuals be published on a publicly available website? This is further complicated by the potential for older students to withhold consent even though their parents/guardians may have given their consent at enrolment.

If the primary purpose/secondary purpose and the need to seek consent seems like an absolute minefield, the rule of thumb is: if in doubt, seek consent.

9. Disclosing Personal Information Outside of Australia

When a school sends personal information overseas, for example when students are going on overseas excursions or exchanges, the school remains accountable for ensuring the information is protected to a level at least equivalent to Australia's Privacy Act requirements.

Under APP 8, before the information is sent overseas, the school must take reasonable steps to ascertain whether there are privacy laws with equivalent or higher protections in the country where the information will be held or used. If that is not the case, then the school must take reasonable steps to erect those protections. For example, a school would be expected to have enforceable contractual provisions requiring privacy protection with penalties for non-compliance in place. The school is required to notify individuals that their personal information is being sent overseas, and to which countries.

Where the school is not confident of either the legal privacy protections in the country or that a contract would be sufficient, it must seek consent from individuals to send the information overseas. When obtaining an individual's consent, the school must tell them that the overseas recipient may not be accountable under Australia's privacy regime and that the individual may not be able to seek redress in case of a breach. The school must also inform the individual of any other potential consequences.

Where the school uses servers outside Australia through which personal information is stored or passed, this information should be included in any collection notice and the school's Privacy Policy.

10. Direct Marketing Restrictions

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 impractical to obtain consent with respect to each direct marketing communication (which it usually is), a school can still use personal information for direct marketing purposes if they provide, on their website and in each of their communications, a simple, prominent statement that tells individuals how to "opt- out" of receiving further direct marketing communications. The school must comply with the request to opt out.

11. Keeping Personal Data Secure

It is fairly self-evident that an organisation must keep personal information securely. This is reinforced by APP 11 and the Notifiable Data Breach scheme, both of which include penalties arising out of data breaches where the organisation failed to take reasonable steps to protect data.

Even a cursory risk assessment will identify a large number of areas where there can be accidental or unauthorised access or interference with personal information as a result of human error: loss of laptops, smart devices, USBs or hardcopy files which hold student or parent information, sending sensitive emails or providing personal information over the phone to the wrong recipient. Then there are the more deliberate breaches such as hacking, theft, and misuse of information accessed by staff, which also need to be addressed.

An area which is frequently overlooked is managing the disposal of personal information. Under the Privacy Act an organisation is required to either destroy or de-identify data it no longer needs. Data which has been de-identified is no longer covered by the Act, but if de-identification is not a reasonable option, the school must take steps to ensure that appropriate security bins or shredders or other secure disposal means are available, as well as wiping data when disposing of electronic equipment.

Once these risk scenarios are identified, the school must consider the reasonable steps that it can take to protect the data. And while there are the obvious measures such as password protection on electronic databases and ensuring physical security of hard copies of personal information, the area where the greatest impact can be achieved is by embedding a culture of privacy and security amongst staff. Each part of the school should identify what steps it can take to protect the data it holds. These steps can then be added to whole school policies and training programs so that all staff can maintain privacy and IT security and operate internally on a "need-to know" basis.

12. Notifiable Data Breaches

Changes to the Privacy Act in 2018 make it compulsory for schools to notify affected individuals and the regulator (the OAIC) if there is a data breach which is likely to cause serious harm to any individuals whose personal information has been disclosed. The serious harm can be physical, psychological, financial, emotional or reputational. A data breach occurs where:

> ***"Personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference."***

Where the school becomes aware of a data breach, which may be a lost or stolen laptop, hacked databases, mis-sent email, or other, it must immediately set in chain procedures which include taking any reasonable remedial measures and assessing the likelihood of serious harm to the individuals whose data has been affected. If the remedial action is insufficient to prevent serious harm to some or all of the affected individuals, then the school must notify the individuals and the OAIC. There are strict rules regarding the methods the school must take in order to bring the breach to the attention of the individuals, with monitoring by the OAIC.

There are penalties under the Privacy Act if the school has failed to comply with the notification requirements and further penalties may arise if the breach resulted from inadequate measures taken by the school to protect the personal information that it holds. The school must have procedures in place (Data Breach Response Plan) and someone to co-ordinate the response (such as a Privacy Officer and Data Breach Response Team).

For further information see our White Paper ***Privacy: Mandatory Notification of Data Breaches***.

13. Individual Rights: Integrity of Data, Access, Amendments, Queries and Complaints

Under APP 10, the school must take reasonable steps to ensure that the personal information it holds is "accurate, up-to-date, complete and relevant".

There are a number of aspects to this requirement, and it touches on a number of the APPs. In terms of information workflow, the first aspect is that the information being collected is accurate and only collected if it is necessary to fulfil the purposes for which it is being collected. In most cases this means obtaining it from the individual, and not collecting unsubstantiated rumours. This is particularly relevant when assessing job applicants, where great care should be taken in determining which comments from a referee should be recorded. In the interests of fairness, where negative comments are made about a job applicant, consider raising the issue with the applicant and asking them to comment.

Once the information has been collected, the school should have procedures in place to review the currency and accuracy of the information it holds. In relation to student data this most often means sending out regular reminders to parents/guardians to update information, which is particularly important with records of emergency contacts and medical/health information and where there are court orders in place. It may also be appropriate to update consents for use of personal information, for example for publication of student information on the school's website, and consider including students in the discussion when seeking consent from their parents/guardians, particularly if the student is of an age where it is reasonable to assume they have the capacity and maturity to make those decisions.

Where a school updates information it is incumbent on the school to then ensure that it advises any parties to whom it provided the original information, of the updates.

A central compliance obligation under the APPs is that a school's Privacy Policy must include information on how individuals can seek to access and/or amend personal information about them (or their child). This is an important way of ensuring the accuracy of personal information. However, it is not without risks. For example, access to the requesting person's personal information may breach another person's privacy. The school is required to have a procedure setting out how this process of access and amendment will be managed, keeping in mind that the Privacy Act sets out the circumstances when a school may refuse access to some or all information, and how it can manage situations when it does not agree with the amendments sought by the individual.

Also bear in mind that the school must include a privacy complaints mechanism that is readily accessible by individuals. And an important point to note is that under APP 2, individuals have the right to interact with the school anonymously or under a pseudonym if "reasonably practicable". While this clearly would not be practical in most

interactions with a school, it may arise in the area of complaints. Anonymous complaints can be problematic because the anonymity limits further investigation and the capacity to provide feedback. However, it would not be appropriate to dismiss all anonymous complaints for that reason. Note that the right to make anonymous complaints is not restricted to making complaints relating to privacy.

It is clear that requests for access, amendments, and complaints can be particularly sensitive, so it is critical that all school staff know how they should be managed. Having clear procedures and training for staff are essential. Also, nominating a Privacy Officer to be the first point of contact, and developing their expertise, will enable these issues to be addressed in a compliant and consistent manner, and hopefully prevent escalation.

14. Students and Privacy

For schools the question arises of whether consent should be obtained from a student's parents or directly from students themselves when collecting personal information. It also raises even more controversial issues in relation to disclosure of personal information, particularly sensitive information. Schools have generally proceeded on the basis that because parents generally have the right to make decisions for their children until they reach 18 years of age, and schools have a direct contractual relationship with a student's parents, notifications provided to parents will act as notifications to students and consent received from parents will act as consent given by students.

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. The only guidance is that the individual must have "capacity to consent" to decisions relating to the privacy of their personal information. The privacy regulator, the OAIC, has advised that if the individual is under 18 years the school must decide on a case-by-case basis whether they have the capacity to consent. Where a case-by case procedure is not practical, the organisation may assume that an individual over the age of 15 has capacity to make such decisions. The proviso here is that if the school is unsure whether a 15- to 17-year-old student has the capacity to consent, they can include the parent/guardian in the discussion.

For practical purposes this rule of thumb is more likely to mean that while the school will be communicating directly with parents/guardians in many cases, it should definitely start including older students in communications regarding their personal information.

While they may find the prospect tempting, a student is probably not able to direct the school to withhold educational information from their parents/guardians, even if the parents/guardians are non-custodial.

However, when it comes to non-educational personal information and sensitive information such as health-related matters, the school's duty of care to the child becomes an important criterion in deciding which information, and how much, to disclose. The school will need to consider the age and best interests of the student as a key starting point, as well as their expectations about who will access the information, and the actual need for the parents/guardians to be informed. These competing considerations are likely to come to the fore in situations where an older student does not consent to sensitive information being disclosed to their parents.

15. Exemption of Employee Records

The school's handling of employee records is exempt from the Privacy Act provided those records directly relate to a current or former employment relationship. If the information is used for a purpose not directly related to the employment relationship, for example giving out the information to a marketing company or a superannuation company seeking new clients, this is not considered to be directly related to the employment relationship and so would be covered by the Privacy Act.

Personal information relating to job applicants is not exempt from the APPs; it is only once an applicant becomes an employee that their records are exempt. This means that the sensitive area of referee reports and the school's internal selection documentation relating to the individual are potentially open for the applicant to request to access and correct. APP 12 provides limits on what the applicant can access, and this will also be affected by the information sharing legislation that is being passed in a number of states and territories in relation to child safety information.

Even though the Privacy Act does not cover employment records directly related to the employment relationship, there are a number of other laws which provide employees with protection, such as occupational health and safety and workers compensation legislation, surveillance legislation (computers, CCTV, telephones, tracking), and rights to access some information (pay, superannuation, leave) in the Fair Work Act 2009 (Cth). It is also worth noting that the Fair Work Commission's interpretation of what constitutes an employment record that is within the Privacy Act may be broader than a more ordinary understanding of the exemption.

16. Appointing a Privacy Officer

A school with 1,500 students will have approximately 3,000 parents, potentially 3,000 prospective parents and 10,000 alumni, meaning that it may hold the personal records of 15,000 to 20,000 individuals. Sheer volume means that it is not a matter of "if" but "when" a privacy query, request to access and amend information, incident, complaint or breach occurs.

In these circumstances, it is incumbent on a school's executive to ensure that at least one person at the school has a good understanding of the Privacy Laws and takes the lead in ensuring that the school is compliant. While the Privacy Act does not mandate this position, nominating an existing staff member to also be the Privacy Officer will provide a first point of contact, both internally and externally, for all privacy matters related to the school.

The Privacy Officer would also be 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 the school's obligations under the Privacy Act. This role would also take the lead in the school's response to any data breaches, including co-ordinating the Data Breach Response Team and communicating with the regulator.

17. Credit Reporting

In some cases, schools may be considered to be credit providers under the Privacy Act, potentially in the context of providing credit with interest in repayment of outstanding school fees, although there may be other scenarios.

Schools that are credit providers are required to implement policies and procedures in accordance with the Privacy (Credit Reporting) Code 2014 (Cth) which supplements the credit reporting provisions in the Privacy Act and Regulations, as well as the more general application of the APPs. The Code seeks to balance individuals' interest in protecting their personal information with the need to ensure that credit providers have sufficient information available to assist them to decide whether to provide an individual with credit.

Legal advice should be sought where this may be a matter for concern.

18. Privacy Does Not Operate in a Vacuum

Compliance with privacy laws requires considerably more than a school simply publishing a "Privacy Policy" on its public website or putting a Privacy Collection Notice on a form. The Privacy Laws require a school to incorporate privacy compliance into its existing governance infrastructure and into its day-to-day operations. A school should:

- ✓ 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 **password protection**, **confidentiality**, **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 in managing personal information
- ✓ ensure it has a functional **Complaints Handling/Incident Management Program** through which it is able to capture and manage privacy enquires or complaints
- ✓ ensure that it has a **Data Breach Response Plan** and all staff understand the types of events (breaches) which would trigger the plan and what they should do about them
- ✓ use its **Risk Management Program** (if a school has one) to identify key privacy-related risks, assess them and effectively control them
- ✓ 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.

For a school to comply with the Privacy Act it is critical that all staff understand and fulfil their roles in protecting personal information. This involves not just the electronic and physical aspects of privacy protection but ensuring that staff are aware of what they can say to whom, the concept of "need to know" when sharing information internally, and when to seek assistance or advice from the Privacy Officer. In many schools this will entail a cultural shift where being helpful must be tempered with respecting the privacy of personal information.

19. Privacy Compliance Checklist

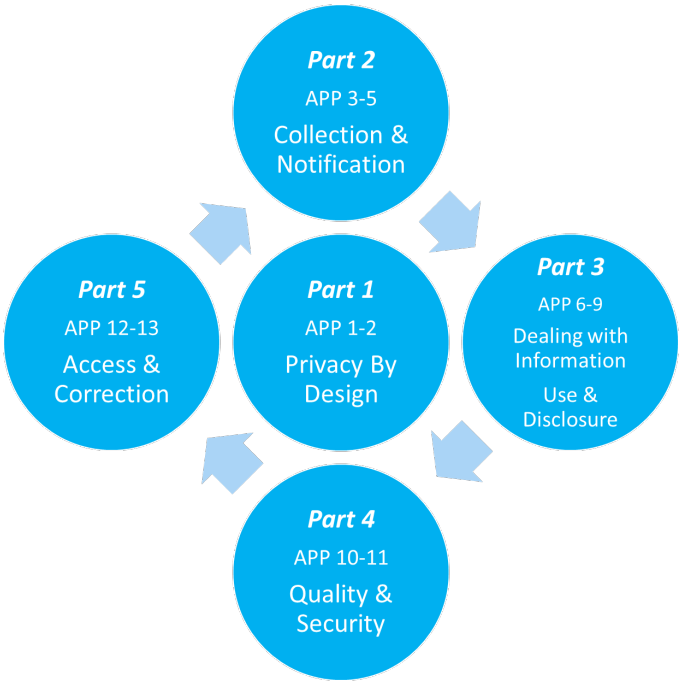
Here's a list of things to do in order to ensure that your school is compliant with its privacy obligations.

Task	Completed
Document your school's Privacy Program (why, what, how, who, when)	☐
Tailor your Privacy Policy to ensure that it fits your school's approach to managing your privacy obligations and publish it on your website and any other appropriate site	☐
Appoint a Privacy Officer and publicise their role to the school community	☐
Complete your Personal Information Management Audit, reviewing your personal information management and security practices, systems and procedures, and close any gaps	☐
Train (and regularly refresh) your staff on privacy practices and obligations	☐
Ensure all information collection forms include a tailored and compliant Privacy Collection Notice	☐
Ensure all direct marketing communications set out clear "opt out" provisions	☐
Ensure that your complaints (including provision for anonymous complaints) and incident management systems are accessible and working	☐
Have procedures in place to ensure that the personal information you hold is accurate and up-to-date	☐
Ensure you have established your Data Breach Response Plan and all staff understand what constitutes a data breach and what to do about it	☐
Ensure personal information which is no longer required, whether in electronic or hard copy formats, is either de-identified or destroyed securely	☐
Establish practices, systems and procedures to ensure your school's ongoing compliance with your privacy obligations through a Compliance Program	☐
Ensure that your Privacy Program is being monitored and regularly reviewed, including your staff's understanding of their privacy obligations	☐

20. The 13 APPs

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 that 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.
Part 2 - Collection and 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 that 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 after collection) schools must take reasonable steps to notify an individual about, or ensure that an individual is aware of, the specific purpose for which their personal information is being collected, and include other prescribed information.

Part 3 – Dealing with Personal Information Use and 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" (both as defined in the Privacy Act) 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 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" (such as Medicare or tax file numbers) as the basis for its own identifier of an individual unless an exception applies.
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 on 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.

How CompliSpace Can Help?

As a leading provider of Governance, Risk, Compliance and Policy (GRC&P) programs and consulting services to a variety of organisations across a range of industry sectors, including over 650 non-government schools across Australia, CompliSpace is here to help.

We enable non-government schools to meet their legal and regulatory obligations and to manage risk, compliance, policies, excursions and staff professional development in critical areas including school registration, human resources management, work health and safety, student duty of care, privacy, child protection, whistleblower, boarding and overseas students.

CompliSpace also publishes ***School Governance***, the Australian school sector's leading news and information source on issues related to governance, risk management, compliance and policy management. It's a weekly newsletter and searchable reference site dedicated to providing unbiased news that relates to the management of schools.

For more information visit **www.complispace.com.au** or call 1300 132 090.

Disclaimer

The information in this White Paper is current as at October 2019. Please visit **www.complispace.com.au** to ensure that you have the most up-to-date version of this White Paper.

