APP Compliance Checklist

This checklist has been prepared by Norton Rose Fulbright Australia, in conjunction with CyberHound Pty Ltd, as a guide to assist schools bound by the *Privacy Act 1988* (Cth) to comply with the Australian Privacy Principles (**APPs**). In some cases, compliance with the APPs will require detailed planning, preparation, training and changes to procedures, practices and forms. Please see the separate detailed checklist relating to the requirements under the APPs for privacy policies.

Note that additional and different rules apply in respect of sensitive information. Sensitive information includes health information and information about an individual's race, political or religious beliefs and other matters. If your school collects or manages sensitive information, you will need advice in addition to the guidance given throughout this document.

Privacy Policy	
Do you have an up-to-date policy regarding the collection and management of personal information and a procedure to periodically review the policy? *Refer to APP 1.3*	☐
Does your privacy policy contain the following information: • the kinds of personal information you collect • how you collect and hold personal information • the purposes for which you collect, hold, use or disclose personal information • how an individual may seek access to personal information held by you or seek correction of such information • how an individual may complain about the breach of an APP, or a registered APP code (if any) that binds the entity, and how you will deal with such a complaint, and • whether you are likely to disclose personal information to overseas recipients and if so, the countries in which such recipients are likely to be located, if it is practicable to specify those countries in the policy. *Refer to APP 1.4*	☐

Have you made reasonable steps to make your privacy policy available free of charge and in an appropriate form, such as on your website? *Refer to APP 1.5*	☐
If requested, are you able to give a copy of your privacy policy in the particular form requested (e.g. a printed copy) by an individual or body? *Refer to APP 1.6*	☐
Identification	
When dealing with individuals, do you provide them with the option of not identifying themselves or using a pseudonym? This does not apply if it is impracticable to deal with individuals who are not identified or where your organisation is required or authorised by law to deal with identified individuals. *Refer to APP 2*	☐
Collection of personal information	
If you collect personal information is it reasonably necessary for one or more of your organisation's functions or activities? *Refer to APP 3.1 and 3.2*	☐
Is the information collected by lawful and fair means? *Refer to APP 3.5*	☐
Do you collect sensitive information? Sensitive information includes health information and information about an individual's race, political or religious beliefs and other matters. You must not collect sensitive information unless you are covered by one of the exceptions in APP 3.3 or 3.4. *Refer to APP 3.3 or 3.4*	☐
Do you collect personal information about an individual **only** from the individual themselves (unless it is unreasonable or impractical to do so)? *Refer to APP 3.6*	☐

Unsolicited personal information	
If your organisation receives unsolicited personal information, do you have in place a process: • to determine whether you could have collected the same information under APP 3 if you had asked for it? • if not, to destroy the unsolicited information as soon as practicable and lawful to do so? *Refer to APP 4.1 & 4.3*	☐
Notification	

At or before the time your organisation collects personal information (or as soon as practicable afterwards) do you provide the individual with the following details? Note that most of these details should be contained in your privacy policy:
• the name and contact details of your organisation
• the fact that you have collected the personal information about an individual if it is likely:
  ○ you collected the information from another source, or
  ○ the individual may not be aware you have collected the information
• details of any law or court order that requires or authorised the collection of the personal information
• the purposes for which you have collected the personal information
• the consequences (if any) if the personal information is not collected
• any other person or entity to whom it may be likely that the personal information will be disclosed
• that your APP privacy policy contains information on complaints and how such complaints will be handled
• whether the personal information is likely to be disclosed overseas
• if overseas disclosure is likely, the countries in which the disclosure is likely to occur.
Refer to APP 5
	☐

Use of personal information	
Do you ensure that your organisation only uses the personal information collected from an individual for the primary purpose for which that personal information was collected unless: • you have consent from the individual for the other purpose, or • the individual would reasonably expect you to use or disclose the information for a secondary purpose that is related to the primary purpose • the use or disclosure is required under law or court order • you reasonably believe that the disclosure is necessary for an enforcement related purpose, or • the use or disclosure is permitted by an exception under APP 6.2 or 6.3? *Refer to APP 6.1, 6.2 and 6.3*	☐
If you disclose personal information for enforcement related activities by an enforcement body (e.g. the police), do you make a written record of that disclosure? *Refer to APP 6.5*	☐
Direct marketing	
Do you have measures in place to ensure that you do not use or disclose personal information for the purpose of direct marketing unless an exception under any of APP 7.2 to 7.5 applies? *Refer to APP 7.1*	☐
If your organisation relies on APP 7.2 to send direct marketing, does your organisation provide a simple opt-out system that includes actually complying with opt-out requests?	☐

If your organisation relies on APP 7.3 to send direct marketing, does your organisation: • make reasonable efforts to obtain the individual's consent, and • ensure that it provides a simple opt-out system;,and • ensures that every direct marketing communication includes a prominent statement about opting-out?	☐
Does your organisation have a system in place to implement each of the following requests from individuals: • that they not receive direct marketing communications • that their personal information is not used or disclosed for the purposes of facilitating direct marketing by other organisations, and • that the source of the personal information collected about them is disclosed? In complying with the above requests, do you also ensure that: • you do not charge an individual for making a request or giving effect to the request • that you give effect to a request within a reasonable time, and • if a request is in relation to the source of an individual's personal information, that the source of that information is revealed to the individual, or should revealing the source of the individual's personal information be either impracticable or unreasonable, that the individual is notified of this within a reasonable time? *Refer to APP 7.6*	☐ ☐
Cross-border disclosure of personal information	
Before disclosing personal information to an overseas recipient, do you take "such steps as are reasonable in the circumstances" to ensure that the recipient does not breach the APPs? *Refer to APP 8.1*	☐

If you not have taken those steps, can you rely on one of the exceptions in APP 8.2? *Refer to APP 8.2*	☐
Government related identifiers – adoption, use or disclosure	
Do you ensure that your organisation does not adopt government related identifiers (e.g. Medicare numbers or driver's licence numbers) as a means of identifying individuals, and does not use or disclose them unless the use or disclosure is necessary to verify the individual's identity for the purposes of your activities or functions (or unless some other exception applies)? *Refer to APP 9.1 and 9.2*	☐
Integrity of personal information	
Do you have procedures in place to ensure that all personal information you collect and store is kept: • accurate • up to date, and • complete? *Refer to APP 10.1*	☐
Do you have procedures in place to ensure that all personal information you use or disclose is: • accurate • up to date • complete, and • relevant, having regard to the purpose of the use or disclosure? *Refer to APP 10.2*	☐

Security	
Do you take reasonable steps to ensure that the personal information you store is protected from: • misuse • interference • loss • unauthorised access • unauthorised modification, or • unauthorised disclosure? *Refer to APP 11.1*	☐
Do you delete or de-identify personal information that is no longer required by your organisation for the purpose for which the information was originally collected? *Refer to APP 11.2*	☐
Access	
Do you have a process in place for giving individuals access to personal information you hold about them (unless an exception in APP 12.3 applies)? *Refer to APP 12.1 and 12.3*	☐
When dealing with requests for access: • Do you respond to the requests within a reasonable time? (*APP 12.4(a)(ii)*) • Do you give access in the manner requested by the individual, where reasonable? (*APP 12.4(b)*) • If you refuse a request for access, do you take reasonable steps to meet the needs of the individual in some other way? (*APP 12.5*) • If you charge for access do you ensure that the charges are not excessive and do not apply to the making of the request? (*APP 12.8*) • If you refuse to give access either at all or in the requested manner, do you provide a written notice setting out the reasons for the refusal and information about mechanisms to complain about the refusal? (*APP 12.9*)	☐

Correction	
If you hold personal information that you or the relevant individual believe to be inaccurate, out of date, incomplete, irrelevant or misleading, do you take reasonable steps to correct the information? *Refer to APP 13.1*	☐
If you have disclosed incorrect personal information to another entity, and the individual asks you to notify the other entity of the correction, do you do so (unless impracticable or unlawful)? *Refer to APP 13.2*	☐
If you refuse an individual's request to correct the personal information, do you provide written notification of your reasons for refusal with information about mechanisms to complain about the refusal? *Refer to APP 13.3*	☐
If you refuse an individual's request to correct the personal information, do your systems allow for a statement to be associated with the personal information so that all your users of the personal information can see that the individual claims that the information is incorrect or misleading? *Refer to APP 13.4*	☐
Does your organisation respond to requests for corrections within a reasonable time and ensure that it does not charge the individual for making the request, correcting the personal information or for associating a statement? *Refer to APP 13.5*	☐