

# SCHOOL PRIVACY CHECKLIST

Practical ways to comply with Australian Privacy Law

Schools must comply with the Australian Privacy Principles (APPs) of the Privacy Act 1988 (or those set out in State privacy laws). These Principles help schools manage privacy risks when collecting and handling personal information, including student images. Data Breach Notification requirements also apply where schools bound by the APPs fail to secure personal information from unauthorised access or disclosure. A failure to meet privacy requirements can result in penalties of up to \$2.1 million and, as part of major changes to privacy law in Australia, the Government plans to increase this amount substantially in late 2019/ early 2020. Privacy is a risk that schools can no longer ignore!

**Any questions?**  
Feel free to call us on  
**1300 438 389** or email  
**privacy@pixevely.com**

- ASSEMBLE YOUR TEAM**  
Appoint (or get to know) your Privacy Officer. They will understand the risks associated with handling personal information and assist school leadership with APP compliance.
- SHARPEN YOUR PRIVACY POLICY**  
A good privacy policy will help your school community understand what personal information your school collects & manages, and how it complies with the APP's. Families with privacy concerns/ complaints will need easy access to your privacy policy for guidance.
- BRAINSTORM AT SCHOOL**  
Explore if any administrative or technical practices/activities pose a privacy risk and discuss solutions with your Privacy Officer. Always welcome feedback from your staff at the same time.
- PROMOTE CONTINUED LEARNING**  
Conduct regular training sessions with your staff regarding privacy obligations. Try 'lunch & learn' sessions, online training, webinars or group seminars.
- BROAD AWARENESS**  
Build community awareness of your school's privacy practices. Add a 'Privacy Note' to your weekly newsletter and participate in the annual Privacy Awareness Week.
- COLLECT CORRECTLY**  
If you don't need it, don't collect it! Make sure that your Collection Statement is up-to-date and accessible. All personal information must be collected in accordance with the APP's.
- INVEST IN SECURITY**  
When using cloud-based services & technologies, especially with personal information, ensure your vendors have privacy and security controls in place. You can manage your risk by only using cloud providers that store your data in Australia.
- KEEP YOUR MEDIA USAGE UPDATED**  
Media Usage/photo consent forms are an important part of upholding privacy obligations. Where you must have permission before using, sharing and publishing student images, get consent! Then update that consent regularly - at least once per year.
- NEVER BUNDLE**  
A consent with many layers and no context does not consider the privacy expectations of students and their parents/legal guardians. Have informative documents asking for specific consent, especially when posting/publishing images online.
- STILL UNSURE? ASK, NEVER ASSUME**  
Even when consents are up-to-date, it is still very important to double-check before using, sharing & publishing images where there may be concern over channel used (e.g. social media) or context.