Mandatory data breach plan 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 to comply with the mandatory notification laws.

Identify and audit personal information held by your organisation	☐
Ensure that systems and processes correctly record: • what personal information is held by your organisation • whether the personal information is held by a third party service provider • where the personal information is stored, and • who the personal information is about. It will be difficult to determine whether an eligible data breach has occurred if you are not able to accurately assess the personal information that you hold.	
Implement internal policies and procedures to prevent, detect, manage and internally report on data breaches	☐
These policies should include a: • Data Breach Response Plan, and • Data Breach Notification Plan. A clear and simple internal reporting mechanism will assist in the prompt reporting of suspected data breaches. Existing policies relating to information security, cyber security, business continuity and personal information may also need to be reviewed and updated. In particular, ensure that your policies regarding information security are up-to-date and implemented and have sufficient scope to include security in respect of mobile phones and portable computing devices.	
Rehearse your Data Breach Response Plan	☐
If a data breach occurs, you will have 30 days to determine whether it is an eligible data breach which needs to be notified. This means that your Data Breach Response Plan needs to be responsive, well-rehearsed and directed to facilitating the prompt investigation and assessment of data breaches. In the course of rehearsing the implementation of your Data Breach Response Plan, you will often identify opportunities to update or improve your Plan.	

Consider appointing a breach coach	☐
The role of a breach coach is to provide advice regarding the management of data breaches. The role of breach coaches is flexible and will depend on the nature of the data breach. The breach coach may assist you by verifying that the appropriate steps are being taken to contain or investigate a data breach, or may assist you to manage internal and external stakeholders, or by facilitating the engagement of external investigators and advisors. Given the tight timeframes, it may be useful identify and appoint a breach coach before a data breach occurs.	
Review contracts with service providers	☐
You should ensure that contracts with third party service providers who store, process or manage your personal information include appropriate contractual provisions, for example: • an obligation to promptly notify you of any actual or suspected data breach, and • you have the right to investigate and require cooperation in respect of any actual or suspected data breach suffered by the service provider. The agreement should also make it clear who will be liable for costs associated with a data breach. The service provider's policies and privacy practices should also be reviewed.	
Review data and document destruction and retention policies	☐
The proper and timely destruction of personal information when it is no longer needed by your organisation will reduce the risk of a data breach causing serious harm.	
Consider taking out cyber insurance	☐
Cyber insurance is specifically designed to cover risks, costs and liabilities arising from data breaches.	
Conduct staff training	☐
All staff should be made aware that suspected data breaches must be reported in accordance with internal policies and processes. It is important to make your staff aware that data breaches do not only occur as a result of a malicious act or a cyberattack. The loss by staff of personal electronic devices or hard copy documents could also constitute a data breach.	