Notifiable Data Breach POLICY & PROCESURES

Drafted By:		Business Manager	Status: June 2018	CURRENT
Responsibility:		Management Team	Scheduled review Date:	March 2019
Updated by:			Changes made:	

1. INTRODUCTION

This policy will assist Mumbulla School with enforcing the Notifiable Data Breach (NDB) Scheme under the Privacy Act 1988 (Cth) (Privacy Act). As an independent school, we must now be aware of our new obligations under the Privacy Act and more importantly, understand how to comply with them to prevent and deal with a data breach.

A vast array of personal information is obtained and kept by Mumbulla School about students, former students, parents and staff. For example, contact details, bank details, family information, medical records, photos. For this reason, it is paramount for Mumbulla School to practice privacy everyday to ensure that the collection, storage, use and disclosure of information about all its stakeholders complies with the Privacy Act and the Australian Privacy Principles (APPs).

2. PURPOSE

The purpose of this policy is to establish procedures to enforce the NDB Scheme. The NDB Scheme prevents schools from concealing eligible data breaches if the breach is considered to result in serious harm to the affected person(s). Under section 26WE of the Privacy Act, an eligible data breach occurs where:

- there is an unauthorised access or unauthorised disclosure of information and a reasonable person would conclude that access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
- information is lost in circumstances where such unauthorised access or disclosure is likely to occur and a reasonable person would conclude that, assuming such access or disclosure did occur, it would be likely to result in serious harm to any individuals to whom that information relates.
- For schools, data breaches are not limited to hacking or cyber attacks on school systems. More commonly, data breaches occur due to internal human errors or a failure to follow information handling policies that result in personal information being inadvertently lost or disclosed to the wrong person

Examples of circumstances which may meet the criteria of a NDB, include when:

1) a device containing a member of the school community's personal information is lost or stolen (e.g a school laptop)
2) a database containing personal information is hacked
3) personal information about students or staff is mistakenly provided to the wrong person
4) records containing student information is stolen from unsecured recycling bins, or
5) disclosing personal information about students/staff for purposes other than what it was collected for and without the consent of the affected students/staff.

It is important to be aware that not all breaches will amount to a NDB.

3. POLICY

Aims

Mumbulla School aims to prevent data breaches. We have prepared the undertaken to adhere to the procedures listed below. However, in the case that a data breach does occur, notification as per the below actions will take place.

Responsibilities

It is the responsibility of the Business Manager and the ICT Administrator to ensure that any Notifiable Data Breach are investigated and are handled in a timely fashion and according to this policy.

Non-government schools who are governed by the Privacy Act and APPs may be subject to significant financial penalties for failing to comply with requirements under the NDB Scheme. The financial penalties that can be imposed for non-compliance are:

- $2.1 million for organisations
- $420,000 for individuals.

To avoid these severe financial penalties, non-government schools need to document and implement a Privacy Program.

4. APPLICATION OF THIS POLICY

We seek the co-operation of all workers, students and their families and other persons to adhere to the Privacy Policy.

That policy, as well as this NDB policy, applies to all educational and business operations and functions, including those situations where staff, students and parents are required to work off-site.

If the School determines that there is a suspected data breach, they must investigate it immediately. In the event of a NDB, the school's Privacy Officer will establish a Data Breach Response Team (DBRT). The DBRT is responsible for assisting the Privacy Officer in investigating the breach and notifying the OAIC when required. The DBRT may include members of staff including management, members from the school's IT department and members from other areas of the school as required. The nature of the breach will determine who will form part of the DBRT.

1. If remedial action is taken to contain a suspected data breach and thereby preventing the likely risk of serious harm occurring, and the action is successful, the data breach does not need to be reported.
2. If the data breach cannot be successfully remedied but it is believed that no serious harm could result, the data breach does not need to be reported
3. If you are unsure if the data breach has been successfully remedied or whether serious harm will result, but it is reasonable to suspect that it might, you have 30 days to determine this, before you need to report.
4. Once the School forms the view, based on reasonable grounds, that there has been a NDB, it must:
   - prepare a statement in accordance with the Act, and
   - give a copy of the statement to the Office of the Australian Information Commissioner (OAIC) as soon as practicable after the school becomes aware of the NDB.

   The statement must set out:
   - the identity and contact details of the school
   - a description of the NDB that the school has reasonable grounds to believe has happened
   - the kind/s of information concerned, and
   - the recommendations about the steps that individuals should take in response to the NDB that the entity has reasonable grounds to believe has happened.

5. The School will notify the contents of that statement to the affected individuals (students, parents, staff etc.) as soon as practicable.

   There is an online form that should be completed.

   https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

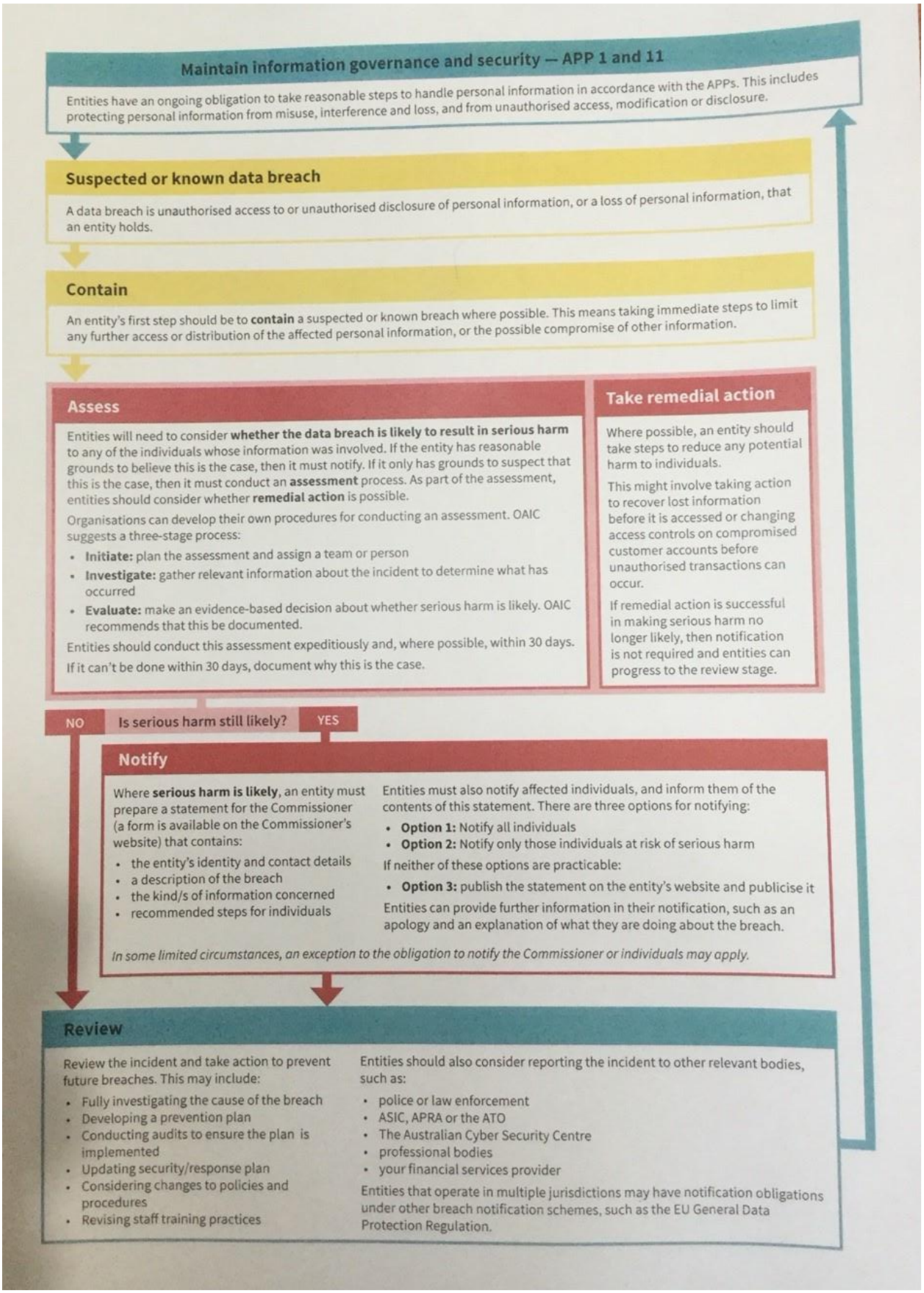
   A Data Breach Response Plan sets out procedures and clear lines of authority for the school in the event that it experiences circumstances that amount to a data breach or a NDB. The response is intended to help the school to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals and to meet NDB obligations under the Privacy Act.

6. Some of the main risk protection measures that the Schools will include in our every day practice:

- Prevention of communication interception e.g. man in the middle attacks, via public unsecured WiFi, Bluetooth, even fake cell phone towers (aka stingrays) which spoof 2G/3G/4G connections.
- Preventing physical device access through tactics such as strong password policies, enforced encryption, geo tracking and geo fencing.
- Ensuring device compliance with policies that are suited for your organisation, industry, and types of device usage. This may include enforced separation of work and personal data and apps, to reduce the risk and liability of the business.
- Ensure personal information access via Facebook, the School will look closely at our cyber security policies to prevent any data breaches from occurring in the future and make sure personal information handling guidelines are clear and all staff are trained in their use.

Appendix A

Notifiable Data Breach Flowchart



Appendix B

The table below lists features of such a Privacy Program

TASK	BY Whom?	Completed
Document a Privacy Program (why, what, how, who, when).		
Appoint a Privacy Officer	Business Manager	
Conduct a Personal Information Management Audit to test the security of personal information protection processes and procedures.		
Ensure all Information Collection Forms include a Privacy Collection Notice		
Ensure all direct marketing communications set out clear "opt out" provisions		
Ensure that our complaints and incident management systems are working		
Review your Privacy Policy to ensure it reflects your approach to managing personal information, including your use of technology to collect or hold personal information	Business Manager	
Create a Data Breach Response Plan to document how your will respond to a Notifiable Data Breach		
Establish a Data Breach Response Team to assist the Privacy Officer in the event of a Data Breach.		
Train your staff on privacy issues		
Publish the School's up-to-date Privacy Policy Reporting Policy on your public website		
Notify key stakeholders if your Privacy Policy and Credit Reporting Policy have been updated.		
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.		

For more information on the requirements of the NDB Scheme and Other Relevant Documentation:

- "Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)" (Data Breach Guide
- http://www.schoolgovernance.net.au/wp-content/uploads/2017/10/Privacy-and-Complaints-Briefing-Paper-Your-School.pdf
- CompliSpace has written a Briefing Paper: Privacy update: Mandatory Notification of Data Breaches & Complaints Handling Update