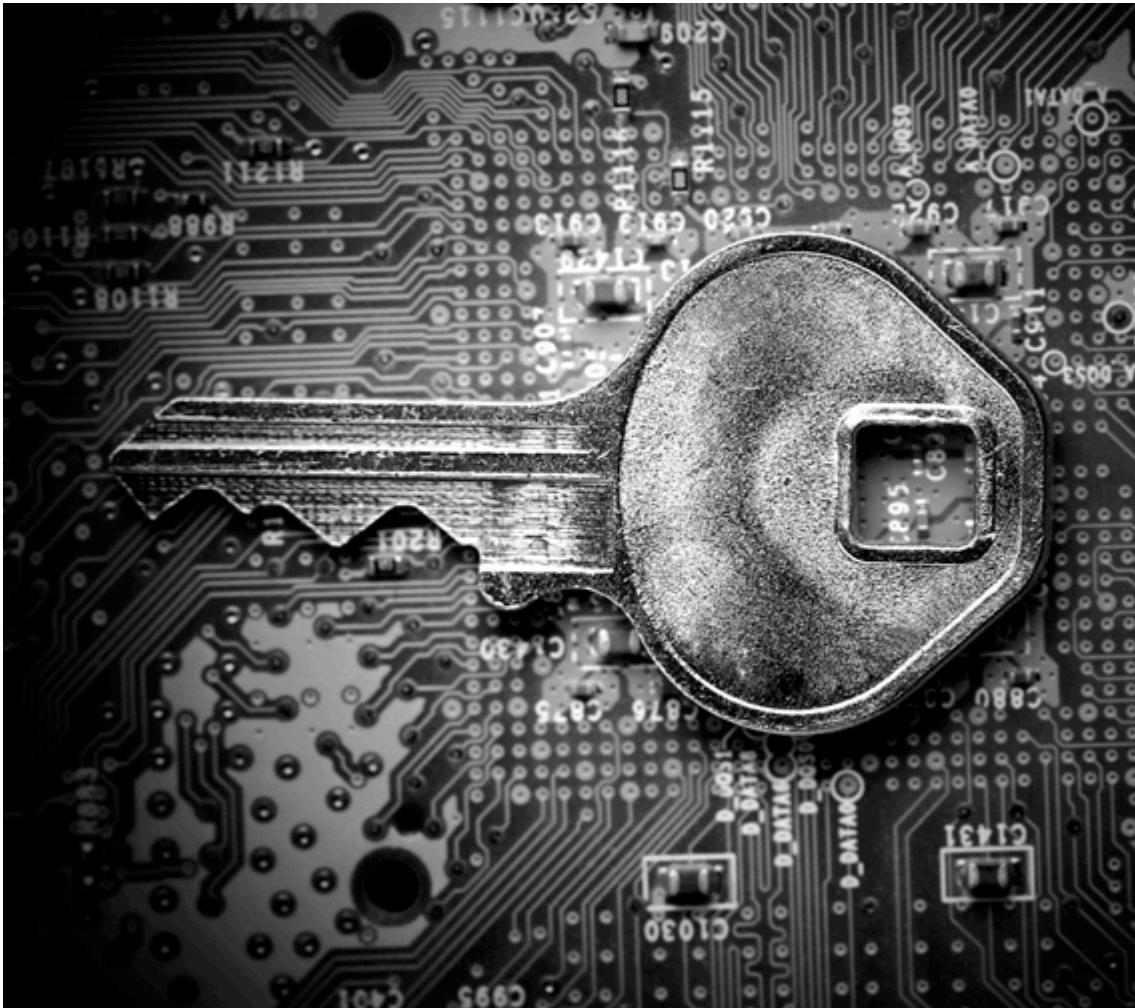


Financial institutions  
Energy  
Infrastructure, mining and commodities  
Transport  
Technology and innovation  
Life sciences and healthcare

 **NORTON ROSE FULBRIGHT**

## Privacy compliance manual for schools Prepared for CyberHound Pty Ltd



**Norton Rose Fulbright Australia**

**April 2018**

**Marshall Bromwich**

Partner, Brisbane

Tel: +61 7 3414 2829

Email: [marshall.bromwich@nortonrosefulbright.com](mailto:marshall.bromwich@nortonrosefulbright.com)

[www.nortonrosefulbright.com](http://www.nortonrosefulbright.com)

## Contents

Scope of this manual.....	3
Data breaches in Australia .....	4
Overview of privacy obligations .....	5
Mandatory notification of data breaches.....	7
Determining whether to notify.....	8
Practical implications .....	9
What steps should you take? .....	12

## Scope of this manual

In general, organisations with an annual turnover of greater than AU\$3 million must comply with the 13 Australian Privacy Principles (**APPs**) prescribed under the *Privacy Act 1988* (Cth) (**Privacy Act**). The APPs deal with how “personal information” is to be collected, handled and disclosed under the Privacy Act.

With effect from 22 February 2018, a new regime for mandatory data breach notifications was introduced under the Privacy Act. Data breaches affecting personal information must now be investigated to determine whether there is a mandatory obligation to notify affected individuals and the Privacy Commissioner.

The majority of independent and Catholic schools in Australia will be caught by the operation of the Privacy Act. Although State schools are not currently caught by the Privacy Act, they may have separate obligations under State-based laws and they still have certain risks if personal information is not appropriately secured. This guide is intended to provide useful guidance in appropriate management of information held by schools, even if the Privacy Act does not apply.

Schools hold a substantial amount of information in their student information systems and other systems and databases, including:

- student and guardian names, date of birth, home address and contact details
- academic records, report, cards and timetabling
- medical records
- BSB and account details of parents paying fees by direct debit, and
- donors and donation amounts.

Schools also hold a substantial amount of information relating to their teachers and staff, including tax file numbers and other identifying details.

Norton Rose Fulbright has been engaged by CyberHound Pty Ltd to prepare this manual to assist schools in understanding their obligations in relation to data protection and management.

This manual provides a high level overview of the APPs and data breach notification requirements and provides practical guidelines to assist schools comply with their obligations under the Privacy Act.

### Disclaimer

This publication is not intended as legal advice, nor should it be construed or relied upon as such. Readers should be sure to take their own legal advice on any of the issues covered by this publication. Each set of circumstances will be different and legal advice should be obtained.

## Data breaches in Australia

Security breaches of IT systems are a significant cost and risk to organisations around the world and they are steadily increasing in frequency and severity. The cost to Australian organisations is estimated to be in excess of AU\$1 billion a year.

Direct financial consequences of a data breach include the cost of hiring IT forensic advisers and the cost of credit monitoring services for affected individuals. Indirect financial consequences include loss of reputation and more generally, loss of revenue due to students and families feeling that they are unable to trust an organisation with their personal information.

Data breaches may be the result of an external attack on an organisation's IT systems. In fact, when someone mentions the words 'data breach', this is typically the first thought for many people. However, IT incidents may arise as a result of a number of scenarios, ranging from employee behaviour, either intentional or unintentional, to information being intercepted before reaching an organisation's systems or acquired through fraud. For example, a phishing website designed to look like an organisation's website may lure people into disclosing personal information to the operators of the website who will then fraudulently misuse the personal information.

It is also worth noting that not all data breaches are caused by an IT incident. Data breaches can also occur when physical documents are left in a public area, not properly disposed of, or when physical documents are lost.

The Australian Cyber Security Centre advises that having a data breach response plan is one of the primary means to improve an organisation's security posture, and has reported that 77% of its respondents had a data breach response plan in place with 37% of them regularly reviewing it.

As the chances of a data breach occurring are on the rise, it is increasingly important that all Australian organisations, including schools, have a data breach response plan in place.

## Overview of privacy obligations

The Privacy Act regulates the collection, use, storage and disclosure of personal information in Australia.

Personal information is defined in the Privacy Act 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.”*

The phrase “reasonably identifiable” deals with the concept of data matching. Data matching occurs where data about an unidentified individual is linked or matched with other data with the effect of causing the individual to become identified. This is sometimes called re-identification. The concept of “reasonably identifiable” is important and relevant to any organisation that intends to disclose anonymised or de-identified personal information (e.g. to research or analytics organisations).

The main obligations under the Privacy Act are now found in the 13 APPs in Schedule 1 to the Privacy Act. The 13 APPs are divided into five different parts, according to the different stages of personal information management running from the collection of personal information through to its disposal:

- **Part 1: Consideration of personal information privacy**
  - APP 1 – Open and transparent management of personal information
  - APP 2 – Anonymity and pseudonymity
- **Part 2: Collection of personal information**
  - APP 3 – Collection of solicited personal information
  - APP 4 – Dealing with unsolicited personal information
  - APP 5 – Notification of collection of personal information
- **Part 3: Dealing with personal information**
  - APP 6 – Use or disclosure of personal information
  - APP 7 – Direct marketing
  - APP 8 – Cross-border disclosure of personal information
  - APP 9 – Adoption, use or disclosure of government related identifiers
- **Part 4: Integrity of personal information**
  - APP 10 – Quality of personal information
  - APP 11 – Security of personal information

- **Part 5: Access to, and correction of, personal information**

- APP 12 – Access to personal information
- APP 13 – Correction of personal information

Norton Rose Fulbright has prepared a number of short guides in relation to the APPs including:





- a summary of the APPs /including practical tips for compliance)
- a checklist to assist an organisation to assess its compliance with the AAPs
- prescribed matters that must be specifically addressed in an organisation's privacy policy.

## Mandatory notification of data breaches

Data breaches affecting personal information must be investigated to determine whether there is a mandatory obligation to notify affected individuals and the Privacy Commissioner.

All schools regulated by the Privacy Act are required to publicise and notify certain data breaches that they suffer.

### At a glance

-  Notification is required when an “eligible data breach” occurs. An eligible data breach is a data breach that is “likely to result in serious harm” to the individuals whose personal information has been lost, or accessed or disclosed in an unauthorised manner.
-  If affected individuals cannot be notified personally (via email or phone for instance) then an organisation must publish a notification on their website and publically via other channels such as the media.
-  Organisations only have 30 days from the date of becoming aware of a suspected eligible data breach to reasonably and expeditiously investigate whether there are reasonable grounds to believe that the relevant circumstances of the data breach amount to an eligible data breach.
-  The notification period of 30 days is a short window of time, as the investigation of data breaches can be difficult, time-consuming and expensive. It is important that all organisations have procedures in place for dealing with a data breach when a data breach occurs.

The new data breach notification regime only applies to those entities that are currently regulated by the Privacy Act (that is, the private sector, Commonwealth public sector agencies, and a small number of other state-owned organisations). This covers personal information, credit reporting information and tax file number information. Existing exemptions, such as the exemption for small business operators with an annual turnover of less than \$3 million, will continue to apply.

### Investigation of data breaches

The new laws adopt a threshold test based on the oddly-named concept of an “eligible data breach”. The first issue to investigate and consider is whether a particular data breach is an “eligible data breach”.

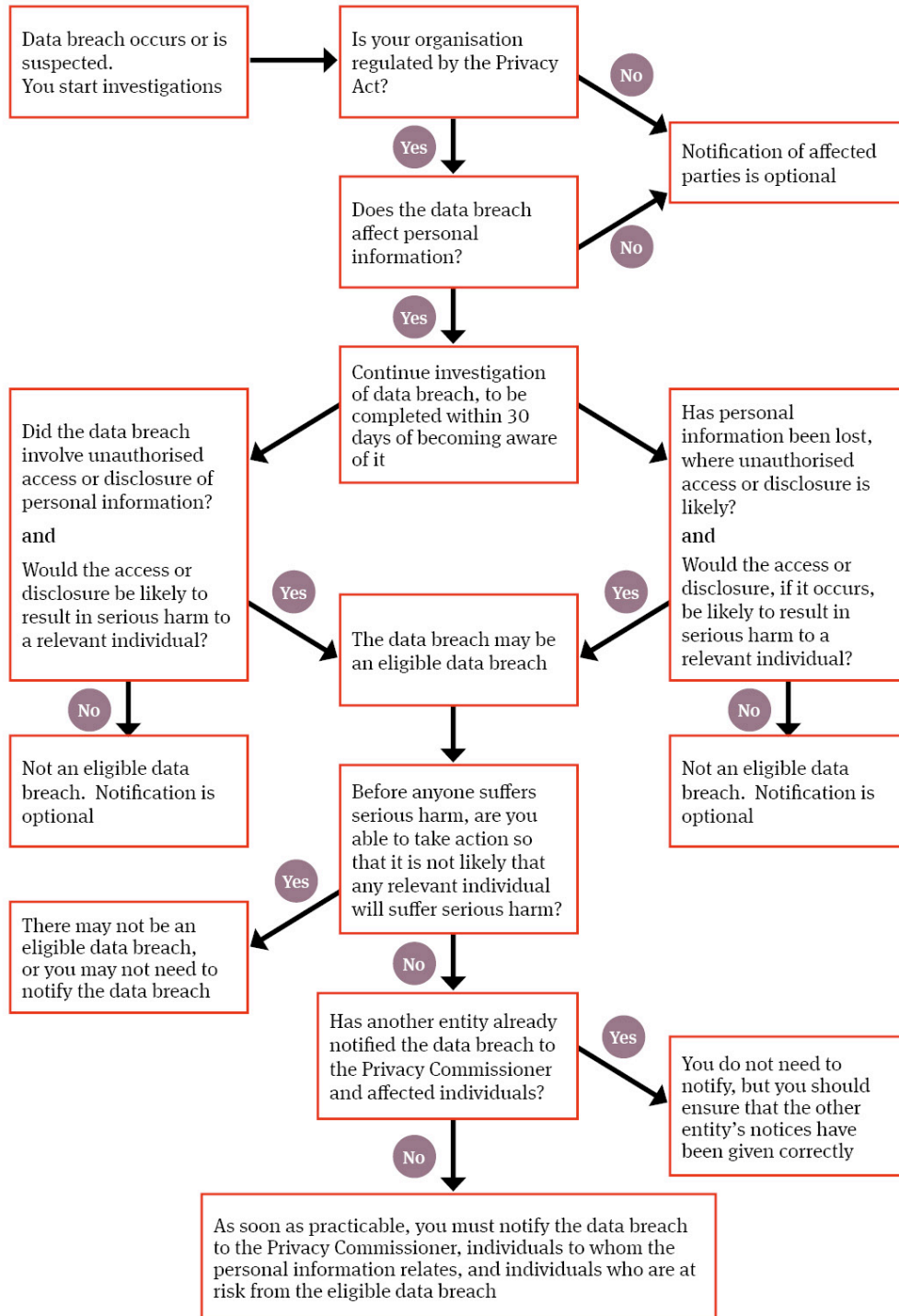
Not all data breaches affecting personal information will be eligible data breaches, as that term is defined in section 26WE(2) of the Privacy Act. This could be because the personal information is trivial, public or otherwise not capable of causing, or likely to cause, serious harm to the individual to whom the information relates. Other exceptions may also apply.

### Timing of the notification

If an organisation or agency is aware that there are reasonable grounds to believe that there has been an eligible data breach, and there are no applicable exceptions to notification, then the organisation or agency must give the requisite notice (which is referred to as a statement in the relevant provisions). The inclusion of the phrase “that there are reasonable grounds to believe” is of significance as it can import a minimum standard on an entity’s ability to detect an eligible data breach. This can have a significant impact on the data management systems and processes of an organisation.

The notice or statement must be given to the Privacy Commissioner as soon as practicable after the organisation or agency becomes aware that an eligible data breach has occurred (section 26WK(2)(b)). The notice must then be given by the organisation or agency to affected individuals as soon as possible after the notice is prepared (section 26WL(3)). The purpose of giving the notification is to assist affected individuals to take steps to avoid or mitigate any harm, loss or damage they may suffer as a result of the data breach. An earlier notification will assist that objective.

## Determining whether to notify





## Practical implications

In order to comply with the new regime, schools regulated by the Privacy Act should consider the following:



- **Identifying and auditing holdings of personal information:** ensure that systems and processes correctly record what personal information is held by the entity, where the information is held and individuals to whom the personal information relates. This is particularly important as it is difficult to determine whether there is an eligible data breach if you are not able to accurately assess what information you hold.
- **Detection and reporting of data breaches:** implement a proper set of internal policies and procedures to prevent, detect, manage and internally report on data breaches (which may include, for example, loss or theft of mobile devices or laptops that may contain significant amounts of personal information, or the improper disclosure of hardcopy records containing personal information). A clear and simple internal reporting mechanism assists the prompt reporting of suspected data breaches.
- **IT Vendor Data Management:** the Privacy Commissioner takes the view that a failure to properly manage a relevant service provider is a failure to comply with the security obligation under Australian Privacy Principle 11.1. For transactions involving the collection, use or disclosure of personal information by an IT vendor or service provider (such as telecommunication, software, infrastructure and hosting providers), a combination of your own due diligence and appropriate contractual provisions is necessary. The contractual provisions could include:
  - the right to audit the vendor's privacy compliance
  - compliance with specified security standards, in addition to any specific requirements, policies or procedures of your organisation
  - an obligation on the vendor to provide an annual report or certification that the vendor has complied with all obligations relating to security and privacy (including notifications)
  - an obligation on the vendor to appoint an independent third party to conduct annual security tests and reviews, with a corresponding obligation to provide a copy of the independent third party's report to you
  - the right to investigate and require cooperation in respect of actual or suspected data breaches
  - the right to appoint third party auditors and investigators to access and review the relevant information, systems and premises of the vendor
  - an obligation on the vendor to cooperate and provide assistance in respect of investigations by the Privacy Commissioner or other relevant regulators.

- **Data destruction and retention policies:** review your data and document destruction and retention policies. Under Australian Privacy Principle 11.2, entities are required to destroy or de-identify personal information when the personal information can no longer be used or disclosed in accordance with the Australian Privacy Principles (typically when the original business purpose has been completed or expired). Personal information that is properly destroyed cannot be the subject of a data breach and the Privacy Commissioner considers that a failure to destroy personal information can lead to, or amount to, a breach of security and of Australian Privacy Principle 11.2.
- **Data Breach Response Plan:** implement and rehearse a comprehensive data breach response plan to deal with all reported data breaches. The response plan should allow for the investigation and assessment that considers that risk of serious harm to the affected individuals in order to determine whether a notification is required. The new provisions in the Privacy Act require entities to use reasonable steps to complete an assessment of a data breach (to determine whether it was an eligible data breach) within 30 days. This means the data breach response plan should be responsive, well-rehearsed and directed to facilitating the prompt investigation and assessment of data breaches.
- **Appointment of a breach coach:** a significant data breach will tend to raise a wide range of issues. The appointment of a breach coach can assist in identification and management of these issues. The role of a breach coach is to assist the in-house staff of an organisation or agency to identify and manage the affected data, to suggest the engagement of key external advisors such as IT forensic specialists, crisis PR teams and to identify issues requiring legal or technical advice. A breach coach who is an external lawyer can also assist the organisation or agency to have the protection of legal professional privilege by engaging some external advisors directly if it appears that legal liability may be an issue. Norton Rose Fulbright is able to play the role of breach coach, and can do so in a flexible way that best suits your organisation and is appropriate to the scale and nature of the data breach. Please contact us if you would like further information.
- **Data Breach Notification Plan:** prepare a notification plan to carry out any mandatory data breach notification under the Privacy Act. This plan may be an independent plan, or may form part of your Data Breach Response Plan. A mandatory data breach notification typically requires communications with large numbers of affected individuals and will require careful coordination. You may need to seek input from a range of external advisors, including:
  - brand managers about the impacts of the notification on your brand
  - IT experts in respect of the nature of the data breach and the current status of the investigations
  - legal advisors in respect of compliance with the Privacy Act and defending against possible claims and liabilities, and preparing for and managing regulatory investigations
  - crisis PR specialists in respect of the content of the notification and scripts developed for call centre staff and customer relations staff and for messages on your website
  - call centre/support desk providers in respect of increasing capacity in the days immediately following notification.

Ideally, you will have previously evaluated the experience and capability of each external advisor, together with their usual rates and terms. Your notification plan can then include the contact details for each specific external provider, so that they can be engaged as early as appropriate.

Your organisation or entity may also wish to consider obtaining cyber insurance. Cyber insurance is a relatively new product on the Australian insurance market, but is rapidly increasing in popularity. Cyber insurance is specifically designed to cover risks, costs and liabilities arising from data breaches that are not generally covered under other types of insurance. In particular, cyber insurance can be very useful in respect of the sometimes considerable costs associated with data breach notifications. As cyber insurance policies differ, you should review the coverage and exclusions in any proposed policy to ensure that it is appropriate to the business activities, structure and foreseeable risks of your organisation or agency.

Obviously, a better alternative to data breach notification is to avoid a data breach in the first instance, which means entities should also take the opportunity to review the security of their systems and networks, and take appropriate action to ensure they are sufficiently robust. Norton Rose Fulbright have prepared a checklist to assist you in taking the necessary steps to ensure that your organisation is ready to comply with the mandatory data breach laws.

## What steps should you take?

In addition to having a compliant privacy policy in place, and a plan for responding to data breaches, other steps that schools should take include:

- ensuring that training is provided to your staff members who deal with personal information – for example, teaching, corporate and admin staff, IT and HR (who may store records of job applicants) – to ensure that they understand the new obligations and any procedures your school may require
- reviewing any contracts that you may have in place that deal with personal information to ensure that they contain provisions that will assist your organisation to comply with the Privacy Act
- reviewing your direct marketing practices and materials, including the availability of ‘opt-out’ mechanisms. Whilst the Spam Act will continue to apply to commercial electronic messages, for any direct marketing material sent out in hard copy you will need to:
  - provide recipients with a simple mechanism for opting out, and
  - ensure that, for some customers, every direct marketing communications includes a statement about opting out, and
- reviewing your cloud computing and outsourcing arrangements, particularly if they involve the disclosure of personal information outside Australia. If an overseas recipient of personal information collected by you breaches any of the APPs, you will be held responsible. As a minimum, we recommend that your relevant agreements contain detailed provisions (perhaps including specific obligations, warranties, audit rights and indemnities) requiring overseas recipients to comply with the APPs.