WHITE PAPER

# Privacy Update: Mandatory Notification of Data Breaches

White Paper for Principals, Bursars, Business Managers and Governors of non-government schools.

*The information in this White Paper is current as at September 2019*

CompliSpace Pty Ltd 1300 132 090
www.complispace.com.au
www.schoolgovernance.net.au

ACT | NSW | NT | QLD | SA | TAS | VIC | WA

Published by:

complispace SchoolGovernance

# About the Author

## Svetlana Pozydajew

Svetlana is a Senior Consultant at CompliSpace. She has over 20 years of experience in strategic and operational human resource management, workplace health and safety, and design and implementation of policies and change management programs.

She has held national people management responsibility positions in the public and private sectors, and is now the content specialist at CompliSpace for HR, general compliance for not- for-profits, and health and safety in schools.

She holds a LLB, Masters in Management (MBA), Master of Arts in Journalism, and a Certificate in Governance for not-for-profits.


 

# Table of Contents

About the Author ..... 2
Svetlana Pozydajew ..... 2
1. Executive Summary ..... 4
2. Background: Purpose of the Notifiable Data Breach Scheme ..... 4
3. What is a Notifiable Data Breach? ..... 5
Serious Harm ..... 5
4. What Needs to Happen When There Has Been a Data Breach? ..... 6
Suspected Notifiable Data Breach ..... 6
Remedial Action ..... 7
Data Breach Response Plan ..... 7
Notifying the OAIC ..... 8
Notifying Affected Individual/s ..... 8
OAIC's Powers in Relation to NDBs ..... 9
5. Preventing Data Breaches ..... 10
6. Next Steps for Schools ..... 10
Policies and Procedures ..... 10
7. Additional Resources ..... 10
8. How CompliSpace Can Help ..... 11
Disclaimer ..... 11


 

# 1. Executive Summary

Commencing on 22 February 2018, changes to the federal Privacy Act 1988 (Cth) make it compulsory for schools to notify specific types of data breaches (Notifiable Data Breaches or NDBs) to individuals affected by the breach, and to the regulator, the Office of the Australian Information Commissioner (OAIC). A data breach occurs where "personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference."

As with most of the provisions in the Privacy Act, the NDB requirements apply to all non-government schools whose annual turnover is over $3 million or who provide a health service*. It does not apply to state and territory government schools (which are subject to local privacy laws).

Not all data breaches will be NDBs. An NDB is defined as a data breach that is likely to result in **serious harm** to any of the individuals to whom the information relates. Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

To comply with the NDB requirements, schools will need to have procedures in place that ensure that data breaches are identified and dealt with as required by the Privacy Act's NDB scheme. These must be integrated into a school's documented privacy program and must include a **data breach response plan.** A key element of an effective data breach response is that staff understand their roles and responsibilities if *any* data breach occurs. Early notification of a data breach may enable the school to implement remedial measures that may avoid a data breach from causing serious harm (and so does not become a *notifiable* data breach) or the measures may reduce the number of people affected.

The NDB requirements highlight the need for schools to have implemented their privacy programs as required by the 2014 changes to the Privacy Act, which established the 13 Australian Privacy Principles (APPs). This means that, if a school has not yet taken steps to ensure that the personal information it collects is managed in accordance with the APPs, the school will be exposed to serious reputational damage if a NDB occurs, as well as the risk of serious financial penalties for breaching the Privacy Act.

To comply with the NDB requirements, schools should start by conducting a **Personal Information Management Audit** to both identify the personal information they hold and then to assess how well the school's processes and procedures protect that personal information. The school must also implement a data plan response plan and ensure that all staff know what their responsibilities are if they become aware of or suspect that a data breach has occurred.

* Advice from the Office of the Australian Information Commissioner is that non-government schools are considered to be health service providers as they hold and use health records (link https://www.oaic.gov.au/privacy/health-information/what-is-a-health-service-provider/)

# 2. Background: Purpose of the Notifiable Data Breach Scheme

The 2014 amendments to the Privacy Act introduced 13 Australian Privacy Principles (APPs) which for the first time applied to non-government schools. Failure to comply with the APPs can result in significant penalties (see our paper The Privacy Laws & Australian Privacy Principles for more information on the introduction of the APPs).

The NDB changes were introduced to give effect to an earlier report of the Australian Law Reform Commission which found that, as more and more information was being held in electronic format, the risk of breaches in security in relation to that data was also greatly increased. The NDB changes also came hard on the heels of some very high-profile data breaches by financial institutions and social media organisations where they failed to notify or greatly delayed notifying individuals whose personal data had been hacked or otherwise exposed.

The amendment closes one of the gaps in the Privacy Act by imposing a requirement on an organisation to notify the individuals whose data was disclosed rather than waiting for an injured party to notice that their data was being misused and then complaining about it. The requirement to also notify the regulator of the breach ensures that the regulator will be able to monitor how the organisation manages the breach including appropriate notification of individuals, and any subsequent mitigation or remediation action.


 

It should also be noted that, while the Privacy Act refers to an "eligible data breach" requiring notification to the individual and the OAIC, the term "NDB" appears to be used almost interchangeably with "eligible data breach" by the OAIC on its website.

While all of the APPs have a role to play in protecting unauthorised disclosures of personal information, APP 11, which requires a school to take "reasonable steps" to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure, articulates the most basic measures that a school must undertake to comply with the Privacy Act. Failure to comply with APP 11 is most likely to lead to personal data being subject to unauthorised access, disclosure or use.

# 3. What is a Notifiable Data Breach?

Not all instances of unauthorised access or use of personal information will come under the mandatory reporting regime effected by the NDB changes.

Under the Privacy Act a data breach must be notified where:

- ✓ there is unauthorised access to, or unauthorised disclosure of, or a loss of, personal information that is held by the school
- ✓ the access or disclosure is likely to result in **serious harm** to any of the individuals to whom the personal information relates; ***and***
- ✓ following the breach, the school has not been able to prevent the likelihood of serious harm to affected individuals with remedial action.

Where the school only suspects that it may have experienced a serious data breach it must quickly resolve that suspicion by assessing whether that data breach has occurred – this should be done as promptly as possible but must be completed within 30 days.

The assessment should cover:

- ✓ whether the data breach actually occurred
- ✓ whether serious harm is likely to result.

If during, or on the completion of, the assessment the school has reasonable grounds to believe that there has been a notifiable data breach, it must promptly notify the individuals and the OAIC.

However, if in the course of the assessment, remedial action is able to be taken that would successfully prevent serious harm to affected individuals, the notification is not required.

Examples of a data breach which may meet the definition of a notifiable data breach include when:

- ✓ a device containing a member of the school community's personal information is lost or stolen e.g. a laptop
- ✓ a database containing personal information is hacked
- ✓ personal information is mistakenly provided to the wrong person.

## Serious Harm

For the data breach to be a NDB, the test is whether, from the perspective of a reasonable person in the position of the school, serious harm to an individual whose personal information was part of the data breach is likely to result from the breach. Serious harm can include serious physical, psychological, emotional, economic or financial harm, as well as serious harm to reputation and other forms of serious harm

The Explanatory Memorandum to the Privacy Act refines the threshold of what constitutes "serious" harm, so for example, although individuals may be distressed or otherwise upset at unauthorised access to, or unauthorised disclosure or loss of, their personal information, this would not in itself be sufficient.


 

To determine the risk of serious harm, the OAIC recommends a rather detailed multi-faceted assessment by a school. In addition to looking at what it knows of the individuals whose information has been disclosed, keeping in mind the kind of information and its sensitivity, a school should also consider the kind of persons who could have obtained the information and their likely intentions in relation to that information. Superimposed on this is the requirement of an assessment of whether, even if the data was disclosed in some way, any security measures were in place, such as encryption, which would be likely to render the data unintelligible to the recipient.

Obvious examples of breaches giving risk to the likelihood of serious harm include hacking a school database which holds information relating to parents' banking or credit card details, or mistakenly confirming a student's enrolment at a school to an estranged parent convicted of family abuse.

# 4. What Needs to Happen When There Has Been a Data Breach?

Where a school becomes aware of *any* data breach the school must:

- ✓ take all reasonably practicable steps to remedy the breach or mitigate the effects of the data breach
- ✓ carry out an assessment to determine the cause and nature of the data breach and
- ✓ whether it is reasonably likely that serious harm may result to any individuals whose information was involved
- ✓ determine whether the remedial action was successful in preventing the likelihood of serious harm.

Where remedial action was not successful in preventing the likelihood of serious harm to affected individuals, then this now becomes a notifiable data breach to be addressed under the terms of the Privacy Act, and the school must:

- ✓ prepare a statement of prescribed information regarding a notifiable data breach that is believed to have occurred and submit the statement to the OAIC
- ✓ contact all affected individuals*
- ✓ review the incident and take action to prevent future breaches.

*Depending on the circumstances it may be appropriate to notify affected individuals as soon as the breach is identified, before notifying the OAIC.

If remedial action was successful in preventing serious harm or, following the assessment, serious harm was not reasonably likely, then the school does not need to notify the individuals or the OAIC.

Where a data breach is *suspected* but not yet known, the school must investigate and assess the likelihood of serious harm within 30 days.

Each of these steps is explained in more detail below.

## Suspected Notifiable Data Breach

If a school suspects a data breach that may cause serious harm may have occurred but this is not certain, it has 30 days to determine whether it is reasonable to assume that the data breach has occurred and whether serious harm is likely to result.

The school should investigate what happened (or might have happened) and evaluate the risks as part of this assessment process. In certain circumstances using external specialists may be considered to assist in the investigation and assessment, for example, in cases of suspected hacking. Remedial action should be considered as soon as enough information comes to light.

The school would be prudent to conduct the investigation and assessment sooner rather than later in the course of the 30 days, as this may enable remedial or mitigation actions to be put in place which may avoid the breach from causing serious harm, or limit the number of individuals who are likely to be seriously harmed.


 

An example of a suspected breach would be where an individual has made a complaint relating to the disclosure of their personal information held by the school. The disclosure may be a one-off mistake by a staff member (which is more easily managed without serious harm) or the complainant could be the first person to notice that hackers have accessed the school's database and have started to use the information. The school should investigate and assess:

- ✓ the circumstances in which the data may have been disclosed
- ✓ any remedial action that can be taken
- ✓ who is likely to be affected
- ✓ whether serious harm will result.

If the assessment reveals that a notifiable data breach has occurred, the school must then follow the notification requirements under the Privacy Act and notify both the OAIC and the individual/s affected.

## Remedial Action

A school should have procedures in place so that, as soon as it becomes aware of any actual or suspected data breach, immediate efforts can be made, where feasible, to remedy the breach to prevent serious harm from occurring or further harm from occurring.

If an unauthorised access or disclosure of personal information occurs but appropriate remedial action is taken by the school, this may avoid triggering the notifiable data breach notification procedures. The test is whether, as a result of that action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals.

Some examples of remedial action which the school may take in relevant circumstances to prevent unauthorised access or disclosure of the information include:

- ✓ An employee has mistakenly emailed personal information relating to one individual to the wrong individual. The school asks the second individual to delete the information without using or disclosing it. The second individual confirms that they have done this, and the school is confident that the second individual has complied with that request.
- ✓ An employee has left their work laptop, which contains large amounts of personal information relating to students, on the bus. The school remotely erases the memory of a lost or stolen device before its contents can be accessed without authorization.

There may be situations where the remedial action is only partially successful. Examples would be where remedial action was triggered after only one of a series of data breaches occurs, so that the risk of serious harm is restricted to a few individuals instead of all of the individuals on a list. If there is a risk of serious harm to the few individuals, this would still constitute a notifiable data breach and the individuals who remained at risk despite the remedial action, would need to be notified (as well as the OAIC). The individuals whose information was protected following the remedial action would not need to be notified.

## Data Breach Response Plan

Given how important it is to take remedial action in the case of a data breach, it is clear that the faster the school is able to respond to a data breach, the more likely it is to effectively limit any negative consequences. To achieve this end, the OAIC recommends that an organisation develops a data breach response plan (DBR Plan) so that, if a data breach occurs, staff will know what needs to be done, how it will be done, and who will do it. While it is likely that each data breach will be different (one hopes) necessitating a case-by-case approach, having a framework and workflow will expedite taking appropriate actions to respond following a data breach, and ensure that any legal obligations are met.


 

A DBR Plan will generally involve the school:

- ✓ containing
- ✓ assessing
- ✓ notifying
- ✓ responding to data breaches to help mitigate potential harm to affected individuals.

The OAIC has produced guidance on developing a DBR Plan which sets out the roles, responsibilities and actions for managing a data breach.

Developing a DBR Plan is not mandatory, however, doing so is an example of taking "reasonable measures" to protect personal information under APP 11.

## Notifying the OAIC

Once a school has reasonable grounds to believe that there has been a notifiable data breach, the school must:

- ✓ prepare a statement in the prescribed format; and
- ✓ give a copy of the statement to the OAIC as soon as practicable after the school becomes aware of the notifiable data breach.

The statement must set out:

- ✓ the identity and contact details of the school;
- ✓ a description of the notifiable data breach that the school has reasonable grounds to believe has happened;
- ✓ the kind/s of information involved in the data breach; and
- ✓ recommendations about the steps that individuals should take in response to the notifiable data breach.

If the school believes that another entity regulated by the Privacy Act is involved in the notifiable data breach, the statement must include information about the other entity/ies.

This notification to the OAIC should occur as soon as practicable after the school has a reasonable belief that it has committed a data breach that is likely to result in serious harm, and that remedial action was unsuccessful in preventing that serious harm.

It should be noted that the OAIC is not only the regulator but can also provide advice on investigating and taking remedial action in cases of data breaches.

## Notifying Affected Individual/s

Where the school has determined that a data breach has occurred and the likelihood of serious harm cannot be mitigated, the affected individuals should be notified as soon as practicable.

While the notification to the OAIC must include a statement of recommended actions in relation to notifying individuals, which implies that the OAIC is notified before the individuals, the school will need to determine whether the risk of harm to individuals is increased if there are delays, and consider notifying the individuals first (or at the same time).

To comply with the NDB notification requirements, the school must determine which individuals to notify. Under the Privacy Act the school has the option to notify:

- ✓ each individual whose personal information was part of the notifiable data breach; or
- ✓ only the individuals who are at risk of serious harm from the notifiable data breach.


 

If neither of those options is practicable, for example, if the school is unable to contact those individuals, then the school must notify more broadly, as guided by the OAIC.

The determination of whether to notify all affected individuals or only those who are at risk of serious harm, is subject to what is "practicable" under the circumstances. This is not defined in the Privacy Act, but the OAIC interprets "practicable" as involving a consideration of time, effort and the cost of notifying individuals at risk of serious harm, given the school's capabilities and capacity.

It would seem sensible to prioritise informing only individuals who are at risk of serious harm over all affected individuals, however, there may be situations where the school will not be able to reasonably assess which particular individuals are at risk of serious harm. This could be the case where it would be reasonable for the school to assume that the data breach will cause some of the affected people serious emotional harm, but not all.

The advantage of notifying the whole group of affected individuals is that it is likely to be simpler for the school rather than having to assess each individual to determine if they would be seriously harmed, and additionally, it will allow the individuals to decide what action each may need to take in response to the data breach. The disadvantage of notifying the whole group is that it may cause unnecessary distress to those who would not be seriously affected.

If directly notifying affected individuals or those at risk of serious harm is not practicable, then the school must take steps which would bring the data breach to the attention of individuals who are at risk of serious harm. The OAIC expects that the school will:

- ✓ publish a copy of the statement submitted to the OAIC regarding the data breach on the school's website, which could be for a period of months; and
- ✓ take reasonable steps to publicise the contents of the statement.

If the publication option is taken, the school should choose the publication channels most likely in the circumstances to be effective in bringing the notifiable data breach to the attention of affected individuals. The OAIC indicates that reasonable steps to publicise the online notice could include ensuring the notice is sufficiently prominent on the school's website, publishing it on the school's social media platforms, or even taking out a print or online advertisement in a publication or website that it would be reasonable to expect the affected individuals to notice. This option may be most appropriate where the breach occurs in relation to former students.

When notifying individuals of a data breach that has affected them, the school must include the contents of the statement submitted to the OAIC. If the individuals are notified before the OAIC, then they do not need to be notified a second time as long as all of the relevant information has been provided.

## OAIC's Powers in Relation to NDBs

If the OAIC becomes aware that reasonable grounds exist to believe that there has been a notifiable data breach at the school and the school has not already done so, the OAIC may direct the school to provide a notification to itself and notify affected individuals. The OAIC can also enforce the conduct of a reasonable and expeditious assessment of a suspected notifiable data breach.

The OAIC may also direct the ways in which the school should publicise the data breach.

Once the OAIC has received the notification of a notifiable data breach, it may make inquiries or offer advice and guidance to the school in response to the way the data breach is being managed. The OAIC may inquire about the adequacy of the actions to contain the data breach where feasible, any steps taken to mitigate the impact of the breach on individuals at risk of serious harm, or the steps taken to minimize the likelihood of a similar breach in the future. The last may involve some level of review to see how the school is complying with the APPs to prevent data breaches.

If an individual complains to the OAIC about how a notifiable data breach is managed by a school, the OAIC has the power to investigate.


 

# 5. Preventing Data Breaches

In our paper The Privacy Laws & Australian Privacy Principles we advised that, in order to comply with the Privacy Act, schools needed to implement internal practices, procedures and systems, integrated within their operational framework, to ensure that they comply with each of the 13 APPs.

A key message we have sought to deliver is that simply publishing a privacy statement on a school's public website is not enough. Practising privacy involves more than just directing staff and other members of a school community to its privacy policy; it requires a "privacy by design" approach covering all aspects of the information being collected and handled by the school.

Given the broad range of personal information (including sensitive information) of thousands of individuals (students, parents, prospective parents, job applicants, alumni, volunteers), we strongly recommended that a school undertakes an audit to identify all of the personal information it collects and then assesses how well it is protected, in order to comply with the APPs. It is critical that all staff understand their own role in complying with the APPs in all of their daily activities, including sending emails, answering phones, talking to parents, and how and where they store personal information, and finally that all staff know exactly what they should do if they believe that a data breach has occurred.

# 6. Next Steps for Schools

## Policies and Procedures

With the introduction of the NDB requirements in the Privacy Act, schools are effectively on notice to ensure that they have developed and implemented a privacy program so that the members of the school community understand how to protect personal information in accordance with APP 11.

If a school has implemented a compliant privacy program, it should take the following steps in order to comply with the additional requirements of the NDB changes:

- ✓ review and test the strength of its security measures that protect personal information and identify any compliance gaps (a **Personal Information Management Audit** can be used for this purpose)
- ✓ review the information in the OAIC's APP 11 Guidance Materials which may assist the school to manage any compliance gaps
- ✓ develop data breach response procedures to ensure that the school responds promptly to any data breach including remedial action, assessments, and notifications required to comply with the NDB obligations
- ✓ communicate the NDB procedures to members of the school community
- ✓ train all staff with respect to their privacy obligations and the NDB requirements.

If a school has been tardy in complying with the APPs, it will be at a much higher risk of data breaches occurring. In order to comply with the NDB requirements, the school will have a higher workload ahead to catch up with implementing the policies and procedures necessary to comply with all of the obligations under the Privacy Act.

# 7. Additional Resources

The OAIC provides guidance for organisations to assist them with complying with the NDB requirements, as well as publishing reports on the operation of the NDB scheme.


 

# 8. How CompliSpace Can Help

CompliSpace works with schools to tailor compliance and risk management systems to a school's individual needs and characteristics, ensuring meaningful compliance with their legal and regulatory obligations.

CompliSpace combines specialist governance, risk and compliance (GRC) consultancy services with practical, technology-enabled solutions. We are the leading provider of privacy law GRC services in Australia, working with leading non-government schools and educational authorities in all Australian states and territories.

Our team of lawyers and industry experts actively monitor changes to relevant laws and standards and deliver a full suite of online policies, procedures and governance programs that enable schools to continuously comply with their legal and regulatory obligations.

In response to the introduction of the NDB scheme, CompliSpace has developed detailed policies and procedures, including a DRB Plan that address the provisions under the legislation. The new policies and procedures are designed to integrate into a school's existing privacy program and be tailored to the particular circumstances of each school. CompliSpace has also developed detailed online privacy training which includes information on the NDB scheme.

If you are looking to update your existing privacy content, contact us on:

T: 1300 132 090 E: contactus@complispace.com.au W: www.complispace.com.au

CompliSpace Media is the publisher of the school governance news site: www.schoolgovernance.net.au

## Disclaimer

This White Paper is a guide to keep readers updated with the latest information. It is not intended as legal advice or as advice that should be relied on by readers. The information contained in this White Paper may have been updated since its posting, or it may not apply in all circumstances. If you require specific advice, please contact us on 1300 132 090 and we will be happy to assist.


 