Nunawading Christian College

Data Breach Response Plan

Document Control

Revision Number	Implementation Date	Review Date	Description of Changes	Prepared By	Approved By
Updated Policy	June 2021	June 2023	Operational	Mark Roberts	School Executive School Council

Data Breach Response Plan

Entity:

For the purpose of this procedure, the corporate entity is Seventh-day Adventist Schools (Victoria) Ltd (ABN: 11106906423) trading as Nunawading Christian College (the School)

Summary.

1. The Notifiable Data Breach (NDB) scheme requires regulated entities to notify particular individuals and the Australian Information Commissioner (the Commissioner) about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

2. Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.

3. Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the Commissioner. There are also exceptions to notifying in certain circumstances.

Serious harm:

The Act does not provide an explicit definition of "serious harm". The Explanatory Memorandum to the Act explains that serious harm could include physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the School's position would identify as a possible outcome of the data breach.

The Explanatory Memorandum also emphasises that although an individual may be distressed or otherwise upset at an unauthorised access to, or unauthorised disclosure of, their personal information, this would not in itself be sufficient to require notification unless a reasonable person in the School's position would consider that the likely consequences for the individual would constitute serious harm.

Third party partners:

During the normal course of business, the School will engage with third party partners (Eg: Synergetic, Google and Microsoft) and will provide certain confidential information under the appropriate provisions of the Australian Privacy Principles (APP's). If that partner is subject to a data breach that meets the definition of an eligible data breach, then it is the responsibility of the third party partner to notify the Australian Information Commissioner and the individuals identified who would be subject to serious harm. The partner does not need to alert the School, but would be expected to do so under provisions of the Service Level Agreement (SLA).

Data breach response plan

This data breach response plan (response plan) sets out procedures and clear lines of authority for the School staff in the event that the School experiences a data breach (or suspects that a data breach has occurred).

A data breach covered by the NDB scheme occurs when personal information is lost or subjected to unauthorised access or disclosure. For good privacy practice purposes, this response plan also covers any instances of unauthorised use, modification or interference with personal information held by the School. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals and entities.

This response plan is intended to enable the School to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the notifiable data breaches (NDB) scheme that commenced on 22 February 2018. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

The plan sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the School to respond to a data breach.

Data breach response process

1. The School experiences a data breach or a data breach is suspected by a member of staff.
    a. The breach may have been identified by the staff member or brought to the attention of the staff member by a stakeholder.
2. The staff member immediately notifies the School Privacy Officer and the Compliance Manager.
3. The staff member will make a record and advise the Privacy Officer of the following:
    a. The time and date of the suspected breach
    b. The type of personal information involved
    c. The cause and extent of the breach
    d. The context of the affected information and the breach
4. The Privacy Officer will:
    a. Determine whether a data breach has or may occur.

b. Determine whether the data breach is serious enough to escalate to the Data Breach Response Team

c. If so activated, the Privacy Officer will alert the Principal, Heads of School, Business Manager and the CEO of ASV..

Note: The Principal will act for the Privacy Officer should he / she not be available.

Data Breach Response Team members

Privacy Officer	Mark Roberts	0419336478	Team Leader
Director of IT Services	Myles Cook		ICT Lead
Compliance	Ben Thomas		Deputy Leader
Principal	Meggan James		Board liaison
Marketing and Comms	Di Cotter		Comms and Media

When should a data breach be escalated to the Data Breach Response Team?

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (the Team).

For example, a school staff member may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled (only relates to internal emails), or if the staff member can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no utility in escalating the issue to the response team.

The Privacy Officer should use his / her discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, the Privacy Officer should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to any of the affected individual(s)?

- Does the breach or suspected breach indicate a systemic problem in the School's processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then the Privacy Officer should call together the available members of the Team.

If the Privacy Officer decides not to escalate a minor data breach or suspected data breach to the response team for further action, the Privacy Officer should:

- send a brief email to the Principal, Business Manager and the Director of IT Services, that contains the following information:
  - description of the breach or suspected breach
  - action taken by the Privacy Officer or reporting staff member to address the breach or suspected breach
  - the outcome of that action, and
  - the Privacy Officers' reasons for their view that no further action is required
- log the incident
- ensure that the breach is noted in the Breach Register

Nunawading Christian College Data Breach Response Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, the response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a human resources adviser.

There are four key steps to consider when responding to a breach or suspected breach.

STEP 1: Contain the breach

STEP 2: Assess the risks associated with the breach

STEP 3: Consider breach notification

STEP 4: Review the incident and take action to prevent future breaches

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, the response team should consider whether remedial action can be taken to reduce any potential harm to individuals.

The response team should refer to the checklist below which provides further detail on each step.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

Following serious data breaches, the response team should conduct a post-breach review to assess the School's response to the breach and the effectiveness of this plan, and report the results of the review to school leadership and the Adventist Schools Victoria (ASV) CEO. The post-breach review report should identify any weaknesses in this response plan and include recommendations for revisions or staff training as needed.

The response team should also consider the following documents where applicable:

- the School's Business Continuity Plan (in draft)
- the School's ICT Disaster recovery plan (in draft)

Testing this plan

Members of the response team should test this plan with a hypothetical data breach annually to ensure that it is effective. As with the post-breach review following an actual data breach, the response team must report to school leadership and the ASV CEO on the outcome of the test and make any recommendations for improving the plan.

Records management

Documents created by the response team, including post-breach and testing reviews, should be saved in the following folder:

- Data Breach Response – reports and investigation of data breaches within the School.
- Privacy Breach register

Reporting

The internal handling of personal information will be an agenda item on the Leadership Committee meetings at least once each quarter and include a report of any privacy complaints against the School and internal data breaches.

Nunawading Christian COllege's Data Breach Response Check List

Step 1: Contain the breach

- ☐ Notify the Privacy Officer, who may convene the data breach response team.
- ☐ Immediately contain breach:
  - ☐ IT to implement the *ICT Incident Response Plan* if necessary.
  - ☐ Building security to be alerted if necessary.
  - ☐ Consider whether the IT systems administrator needs to be advised.
- ☐ Consider whether the team needs other expertise
- ☐ Inform the School Executive, including the Australian Information Commissioner, as soon as possible; provide ongoing updates on key developments.
- ☐ Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the School to take appropriate corrective action.
- ☐ Consider a communications or media strategy to manage public expectations and media interest.

Step 2: Assess the risks for individuals associated with the breach

- ☐ Conduct initial investigation, and collect information about the breach promptly, including:
  - ☐ the date, time, duration, and location of the breach
  - ☐ the type of personal information involved in the breach

- ☐ how the breach was discovered and by whom
- ☐ the cause and extent of the breach
- ☐ a list of the affected individuals, or possible affected individuals
- ☐ the risk of serious harm to the affected individuals
- ☐ the risk of other harms.

☐ Determine whether the context of the information is important.

☐ Establish the cause and extent of the breach.

☐ Assess priorities and risks based on what is known.

☐ Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.

Step 3: Consider breach notification

☐ Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.

☐ Determine whether and how to notify affected individuals. Does the breach trigger the requirements of the NDB scheme – is the breach likely to result in serious harm to any of the individuals to whom the information relates and the School has not been able to prevent the likely risk of serious harm through remedial action. In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals. If the NDB scheme is triggered – a formal notification to the AIC through the OAIC's NDB form should be completed and registered in the incident report. Even if the NDB scheme threshold is not met, would notifying the individuals be appropriate?

☐ Consider whether others should be notified, including the ACSC, police/law enforcement, or other agencies or organisations affected by the breach or can assist in containing the breach or assisting individuals affected by breach, or where the School is contractually required or required under the terms of an MOU, SLA or similar obligation to notify specific parties. (Eg: Insurance partners, financial institutions etc,.)

Step 4: Review the incident and take action to prevent future breaches

- ☐ Fully investigate the cause of the breach.
- ☐ Implement a strategy to identify and address any weaknesses in data handling that contributed to the breach
- ☐ Conduct a post-breach review and report to the Finance and Risk Committee on outcomes and recommendations:
    - ☐ Update security and response plan if necessary.
    - ☐ Make appropriate changes to policies and procedures if necessary.
    - ☐ Revise staff training practices if necessary.