Mernda Hills Christian College

Notifiable Data Breaches Policy

Document Control

Revision Number	Review Date	Implementation Date	Description of Changes	Prepared By	Approved By
Gilson College					
	Aug 2019	Oct 2019	• General review	Exec Leaders	Gilson College Council
Mernda Hills Christian College					
1	May 2023	January 2024	• Thorough review • Added Compliance and Monitoring • Reviewed links	Exec Leaders	Exec Leaders

Document Type: Administrative

Rationale

The purpose of this policy is to ensure that Mernda Hills Christian College is compliant with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the ***Privacy Act 1988*** (Privacy Act). It is understood and accepted that Mernda Hills Christian College has data breach notification obligations when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach.

The policy applies to students and employees, including full-time, part-time, permanent, fixed-term and casual employees, as well as contractors, volunteers and people undertaking work experience or vocational placements, where personal information is stored about these individuals.

Overview

1. Mernda Hills Christian College is committed to ensuring that any personal information that it holds regarding students, parents, employees, or volunteers will be stored securely in accordance with the guidelines from the Office of the Australian Information Commissioner and the existing personal information security obligations under the Australian Privacy Act 1988 (Privacy Act).

2. The passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017 established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme applies to all agencies and organisations with existing personal information security obligations from 22 February 2018.

3. College leadership acknowledges the right of students, parents, employees and volunteers to reasonably expect that its entities will comply with the NDB with regards to investigation, containment, notification, assessment and review with regards to any identified data breaches. Further, it recognises that the NDB scheme strengthens the protections afforded to everyone's personal information and improves transparency in the way that organisations respond to serious data breaches.

Which Data Breaches Require Notification?

1. An 'eligible data breach', which triggers notification obligations, is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Examples of a data breach include when:
   - a device containing personal information is lost or stolen;
   - a database containing personal information is hacked;
   - personal information is mistakenly provided to the wrong person.

2. For more information, refer to the following support documents from the Office of the Australian Information Commissioner (OAIC)
   - Data Breach Notification Guide: a guide to handling personal information security breaches (updated July 2019)
   - Identifying Eligible Data Breaches (July 2019)

Assessing Suspected Data Breaches

1. If any person at Mernda Hills Christian College suspects an eligible data breach may have occurred, the college must undertake reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected. For more information, refer to the following support documents from the Office of the Australian Information Commissioner (OAIC)
   - Assessing a Suspected Data Breach (July 2019)

How to Notify

1. When any person at the College has reasonable grounds to believe an eligible data breach has occurred, the college is obligated to promptly notify individuals at likely risk of serious harm. The Office of the Australian Information Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

2. The notification to affected individuals and the Commissioner must include the following information:
    - the identify and contact details of the organisation;
    - a description of the data breach;
    - the kinds of information concerned; and
    - recommendations about steps individuals should take in response to the data breach. (For more information For more information, refer to the support documents from the Office of the Australian Information Commissioner (OAIC), Notifying Individuals about an Eligible Data Breach (December 2017).

Responsibilities

System Responsibilities:

- See Seventh-day Adventist Schools (Victoria) Limited Notifiable Data Breaches Policy.

College Responsibilities:

1. Mernda Hills Christian College acknowledges its responsibility to ensure the secure storage of personal information in accordance with Privacy Act 1988 (Privacy Act) and the obligation to notify individuals as per the Privacy Amendment (Notifiable Data Breaches) Act 2017 and will undertake the following steps as part of that system governance:
    - Develop, implement, promote and act in accordance with the Seventh-day Adventist Schools (Victoria) Limited Notifiable Data Breaches Policy;
    - Ensure that appropriate support is provided to all parties regarding training and procedures for keeping personal information safe and secure as per the OAIC Guide to Securing Personal Information (June, 2018)
    - Receive from any person related to the college, reports of suspected or known data breaches;
    - Take appropriate action to support the person as they inform them of any eligible data breach;
    - Complete the Notifiable Data Breach Form online to inform the Office of the Australian Information Commissioner on behalf of the entity;
    - Communicate this policy to all staff, students and parents;
    - Assess and reported data breach in accordance with this Seventh-day Adventist Schools (Victoria) Limited Notifiable Data Breaches Policy;
    - Upon identification of a suspected or known data breach, assess the data breach in accordance with the process prescribed in IOAC Identifying Eligible Data Breaches (July 2019) and OAIC Assessing a Suspected Data Breach (July 2019);
    - Take steps to reduce any potential harm to individuals, such as recovering the lost information before it is accessed;
    - As a result of the investigation, notify eligible data breaches to Seventh-day Adventist Schools (Victoria) Limited through the Education Director or IT Manager – Education Services;
    - With the support of the Education Director or IT Manager – Education Services, notify the individuals impacted by the breach of their data with reference to OAIC Notifying Individuals about an Eligible Data Breach (July 2019);
    - Review the incident and take action to prevent further breaches.

Implementation

As part of Seventh-day Adventist Schools (Victoria) Limited (ASV) Mernda Hills Christian College will take reasonable steps to handle personal information in accordance with the Australian Privacy Principles (APP) by:

- only collecting personal information that is reasonably necessary to carry out your functions or activities. Over-collection can increase risks for the security of personal information;
- embed robust internal personal information handling practices, procedures and systems to assist good personal information handling practices and respond effectively in the event a privacy breach occurs;
- conducting a privacy impact assessment, an information security risk assessment and reviews of the Mernda Hills Christian College personal information security controls so that we are aware of the variety of security risks faced, including threats and vulnerabilities, along with the possible impacts before designing and implementing the college personal information security framework;

- implement appropriate security measures to protect the personal information with regards to all of the college's acts and practices;
- take reasonable steps to destroy or de-identify the personal information that was once held but is no longer needed for any purpose.

Compliance and Monitoring

Mernda Hills Christian College, as part of Seventh-day Adventist Schools (Victoria) Limited (ASV) will need to take reasonable steps to handle personal information in accordance with the Australian Privacy Principles (APP):

- Consider whether to collect personal information – only collect personal information that is reasonably necessary to carry out our functions or activities. Over-collection can increase risks for the security of personal information;
- Privacy by design – The College will meet our personal information security obligations by embedding them as robust internal personal information handling practices, procedures and systems and for responding effectively in the event a privacy breach occurs;
- Assessing the risks – The College will conduct a privacy impact assessment, an information security risk assessment, and review our personal information security controls so that we are aware of the variety of security risks we face, including threats and vulnerabilities, along with the possible impacts;
- The College will take appropriate steps and put into place appropriate strategies to protect personal information with regards to all of the Colleges' acts and practices;
- The College will take reasonable steps to destroy or de-identify the personal information that was once held but is no longer needed for any purpose.

Related Policies and Processes

- Privacy Policy
- ASV Privacy Policy
- ASV Notifiable data Breaches Policy

Additional Resources from OAIC

- Data Breach Notification Guide: (July 2019)
- Data Breaches involving more than one Organisation (July 2019)

Relevant Documentation or Legislation

- Commonwealth Privacy Act (1988) Part IIIC
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Guide to Developing a Data Breach Response Plan (July 2019)