NOTIFIABLE DATA BREACH (NDB) POLICY

HALE SCHOOL

1. Purpose

The purpose of this document is to ensure that Hale School meets the standards outlined by the Office of the Australian Information Commissioner in the Notifiable Data Breach (NDB) Scheme and stipulated in the Privacy Act.

This makes it compulsory for schools to notify specific types of data breaches to the individuals affected by the breach, and to the Office of the Australian Information Commissioner (OAIC)

This document sets out the processes to be followed by Hale School staff in the event that the School (or a third-party holding information originating from the School) experiences a data breach or suspects that a data breach has occurred.

Accordingly, Hale School needs to be prepared to act quickly in the event of a data breach (or suspected breach) and determine whether it is likely to result in serious harm and whether it constitutes a NDB. A formal assessment of the data breach is to be completed and submitted to the OAIC within 30 calendar days of becoming aware of the breach.

Adherence to this Policy and Response Plan will ensure that Hale School can contain, assess, and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's "Guide to developing a data breach response plan"
- The Office of the Australian Information Commissioner's "Data breach notification guide: a guide to handling personal information security breaches"
- Notifiable Data Breaches Act

2. Definitions

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."

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures.

Not all data breaches will be NDBs. A 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. 'Individuals' in this context refers to past and current students, parents, staff, and any associates we hold data on.

3. Process where a data breach occurs or is suspected

a. Alert

Where a privacy data breach is known to have occurred (or is suspected) any member of staff who becomes aware of this must, within 24 hours, alert the Head of Information Technology in the first instance.

The information that should be provided (if known) at this point includes:

I. When the breach occurred (time and date)

II. Description of the breach (type of personal information involved)

III. Cause of the breach (if known) otherwise how it was discovered

IV. Which system(s) if any are affected?

V. Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

b. Assess

Once notified of the information above, the Head of Information Technology must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

I. Criteria for determining whether a privacy data breach has occurred

Is personal information involved?

Is the personal information of a sensitive nature?

Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

II. Criteria for determining severity

The type and extent of personal information involved

Whether multiple individuals have been affected. Whether the information is protected by any security measures (password protection or encryption).

The person or kinds of people who now have access

Whether there is (or could there be) a real risk of serious harm to the affected individuals

Whether there could be media or stakeholder attention because of the breach or suspect breach

III. Issue of pre-emptive instructions

On receipt of the communication, the Head of Information Technology will take a preliminary view as to whether the breach (or suspected breach) may constitute a NDB. Accordingly, the Head of Information Technology will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the School's Data Breach Response Team. This will depend on the nature and severity of the breach.

The Response Team will consist of:

- Head of Information Technology
- Director of Learning Technologies (or nominee)
- Director of Community Engagement (or nominee)
- Director of Human Resources and Staff Development (or nominee)

IV. Role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case-by-case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps must be undertaken by the Response Team:

- Inform the Headmaster and Director of Finance and Governance.
- Undertake the assessment within 48 hours of being convened.

The following steps may be undertaken by the Response Team (as appropriate):

- Immediately contain the breach (if this has not already occurred). Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
- Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined in sections 3b.

- Call upon the expertise of, or consult with, relevant staff in the circumstances.
- Engage an independent cyber security or forensic expert as appropriate.
- Assess whether serious harm is likely (with reference to section 3b above)
- Make a recommendation to the Head of Information Technology whether this breach constitutes a NDB for the purpose of mandatory reporting to the Office of the Australian Information Commissioner (OAIC) and the practicality of notifying affected individuals.
- Consider developing a communication or media strategy including the timing, content, and method of any announcements to students, staff, or the media. This aspect is to be coordinated by the Director of Community Engagement.

V. Notification

Having regard to the Response team's recommendation above, the Head of Information Technology will determine whether there are reasonable grounds to suspect that a NDB has occurred.

If there are reasonable grounds, the Head of Information Technology must prepare a prescribed statement and provide a copy to the Office of the Australian Information Commissioner (OAIC) as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

The online form to be submitted to the OAIC can be found here:

https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach

If practicable, Hale School must also notify everyone to whom the relevant personal information relates. Where impracticable, Hale School must take reasonable steps to publicise the statement (including publishing on the School's public facing website).

VI. Secondary Role of the Response Team

Once an incident has been dealt with, the Response team should turn attention to the following:

- Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training.
- Prepare a report for submission to Headmaster, Director of Finance and Governance and Board of Governors.

4. Relevant Legislation

- Privacy Act 1988 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017

5. Related Policies

- Code of Conduct for all Staff
- Information and Communications Technology Policy
- Privacy Policy

Date originally approved:	**Approving authority:**
November 2018	Director of Staff Development and Human Resources
Date this version approved:	**Date policy to be reviewed:**
May 2022	November 2023
Policy Custodian: (Contact for queries)	**Policy Category:**
Head of Information Technology	Information Technology

Policy Version
2
Changes Made
Structure Relevant legislation Related Policies