St Mary
Star of the Sea College
I AM BORN FOR HIGHER THINGS

DATA BREACH POLICY

Date approved	September 2019	**Date amended**	November 2020	**Date of next review**	September 2021
Approved by	St Mary Star of the Sea College Board				
Author	Tony Fitzgerald, Principal				
Responsible body	College Board College Staff				
Supporting documents, procedures and policies	▪ Privacy Amendment (Enhancing Privacy Protection) Act 2012 ▪ Privacy Amendment (Notifiable Data Breaches) Act 2017 ▪ Australian Privacy Act 1988 ▪ Office of the Australian Information Commissioner: a guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth)				
Reference and legislation	▪ Privacy Amendment (Enhancing Privacy Protection) Act 2012 ▪ Privacy Amendment (Notifiable Data Breaches) Act 2017 ▪ Australian Privacy Act 1988 ▪ Office of the Australian Information Commissioner: a guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth)				
Audience	Public - accessible to anyone				

CONTENTS

1. PURPOSE OF POLICY

This policy statement outlines the purpose and procedures adopted by St Mary Star of the Sea College on how personal information is collected and managed in accordance with the Privacy Act 1988, the Privacy Amendment Act 2019 and St Mary's Privacy Policy. This policy sets out the processes to be followed by St Mary's staff in the event that St Mary's experiences a data breach or suspects that a data breach has occurred.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified. Accordingly, St Mary's 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 an NDB.

2. DEFINITIONS

Australian Privacy Principles	There are 13 privacy principles that apply to the handling of personal information.
Data Breach	A data breach happens when personal information is accessed or disclosed without authorisation or is lost. Under the Notifiable Data Breaches scheme, personnel, contractors and suppliers and community members must be told if a data breach is likely to cause them serious harm.
Eligible Data Breach	An Eligible Data Breach occurs when a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals as a result of unauthorised access, unauthorised disclosure or loss.
Privacy Act 2002 (Health Records Act)	This Act promotes fair and responsible handling of health information held in public and private sectors.

3. APPLICATION AND SCOPE

This policy applies to all persons employed in any capacity - school staff, practicum students, parents, students, contractors or volunteers. It also applies to external organisations and their personnel who have been granted access to St Mary's information, infrastructure, services and data. Separate protocols will apply for residents of the European Union.

The scope of the policy includes the College data held in any format or medium (paper based or electronic) that has been assigned a classification of protected for internal use, or confidential. This policy does not apply to information that has been classified as Public. The policy covers all record level and aggregate level data collections within the College, including those provided for by statute. It includes collections of student, staff, parent, corporate and financial information. For the purposes of this policy, data collection includes both operational data collections and data repositories.

POLICY GUIDELINES

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

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

a) When the breach occurred (time and date)
b) Description of the breach (type of personal information involved)
c) Cause of the breach (if known) otherwise how it was discovered
d) Which system(s) if any are affected?
e) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

Assess and determine the potential impact

Once notified of the information above, the Principal or nominee and the Privacy Officer must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. In consultation with the Privacy Officer, the Principal will call together the Response Team consisting of members of the College Executive, the Privacy Officer and other specialist staff as required.

Criteria for determining whether a privacy data breach has occurred:

a) Is personal information involved?
b) Is the personal information of a sensitive nature?
c) 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?

Criteria for determining severity

a) The type and extent of personal information involved.
b) Whether multiple individuals have been affected.
c) Whether the information is protected by any security measures (password protection or encryption).

d) The person or kinds of people who now have access
e) Whether there is (or could be) a real risk of serious harm to the affected individuals.
f) Whether there could be media or stakeholder attention as a result of the breach or suspected breach.

With respect to the above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in Section 26WG of the NDB scheme.

Pre-emptive Action if required
On receipt of the communication the Principal or nominee and the Privacy Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Accordingly, the Privacy Officer will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Response Team.

Where the Privacy Officer instructs that the data breach is to be managed at the local level, the relevant member of the Executive or nominee must:

- ensure that immediate corrective action is taken, 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)
- submit a report via the Privacy Officer within 48 hours of receiving instructions. The report must contain the following:
  - Description of breach or suspected breach
  - Action taken
  - Outcome of action
  - Processes that have been implemented to prevent a repeat of the situation
  - Recommendation that no further action is necessary.

The Privacy Officer will be provided with a copy of the report and will sign-off that no further action is required. The report is then logged.

Data breach managed by the Response Team
Where the Privacy Officer instructs that the data breach must be escalated to the Response Team, the Principal or delegate and the Privacy Officer will convene the Response Team and the Principal who will then notify the Board Chair.

Primary 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 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 above.

- Call upon the expertise of, or consult with, relevant staff in the particular circumstances.
- Engage an independent cyber-security or forensic expert as appropriate.
- Assess whether serious harm is likely.
- Make a recommendation to the Privacy Officer whether this breach constitutes an NDB for the purpose of mandatory reporting to the 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.
- The Response Team must undertake its assessment within 48 hours of being convened.

Notification

Having regard to the Response team's recommendation, the Privacy Officer will determine whether there are reasonable grounds to suspect that an NDB has occurred. If there are reasonable grounds, the Privacy Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

St Mary's must also notify each individual to whom the relevant personal information relates. Where impracticable St Mary's, must take reasonable steps to publicise the statement (including publishing on the website). The prescribed statement will be logged by the Privacy Officer.

Secondary Role of the Response Team

Once the matters have been dealt with, the Response team should turn its attention to the following areas:

- Identifying 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.
- Consider the option of an audit to ensure necessary outcomes have been implemented and are effective.

VERSION CONTROL AND CHANGE HISTORY

Version control	Date effective	Approved by	Amendment
1.0	October 2019	Board	Approval of Policy.
2.0	November 2020	Board	Review of policy. To be merged with Privacy Policy.