BLACKFRIARS
PRIORY SCHOOL

# DATA BREACH RESPONSE PLAN AND PROCEDURES

Date Approved: 2020

Review Date: August 2022

# CONTENTS

## CONTEXT

As the only school founded by the Dominican Friars in Australia, Blackfriars Priory School remains faithful to the search for Truth (Veritas) as lived and taught over the last 800 years by the Order of Preachers (Dominicans), and exemplified by Saint Dominic, our Founder, and Saint Albert the Great, our Patron.

Saint Dominic's commitment to study continued throughout his life. The pursuit of knowledge was not for its own sake but to better understand God's creation and its use in the works of the Order has continued through the centuries. Today, Dominicans can be found throughout the world.

An early member of the Dominicans was Saint Albert the Great. He became a lecturer, scientist, philosopher and Bishop. After his death he was recognised as a Doctor of the Church. The Doctor Universalis – The Universal Doctor, in recognition of his extraordinary genius and extensive knowledge, for he studied every branch of learning known at his time. His quest for knowledge saw him study everything he could find as it was through learning about creation, that he was able to know more about the creator, God, and then hand on that information to all he taught.

The lifelong commitment of Saint Dominic and Saint Albert to discovering and applying Truth to hand on to others remains at the core of the Blackfriars teaching pedagogy and its community. Blackfriars is built upon the Four Pillars of Dominican Life: Prayer, Study, Community Life and Service.

## PURPOSE

The passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (the Act) established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the *Australian Privacy Act 1988* (Privacy Act) from 22 February 2018.

The NDB scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

This document sets out procedures and clear lines of authority for Blackfriars Priory School Staff in the event that the School experiences a data breach (or suspects that a data breach has occurred).

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. 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, agencies and organisations.

The Data Breach Response Plan is intended to enable the School to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals. It 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.

The School manages personal information on behalf of its **customers**. It is important to stress that the data does not belong to the School, it belongs to the customer, and consequently any breach of customer data must be communicated to the customer.

Our standard practice is that the School will never communicate directly with people who are contained in customer data (i.e. Parents/caregivers, Students and Staff) without the explicit permission of the customer. The exception is where, in our view, a notifiable breach has occurred and the School does not have the mechanisms to readily target notifications to the affected people and the School must discharge its obligation under the Act to notify individuals at likely risk of harm.

The School will ask all customers to provide a contact person who will be the customer's liaison with the School in the event of a data breach.

## SCOPE

The Data Breach Response Plan Procedure applies to all members of the Blackfriars Priory School community.

## PROCEDURES

Key Contacts

| Principal | Business Manager |
|---|---|
| Simon Cobiac<br>08 8169 3900<br>principal@bps.sa.edu.au | Gerard Leahy<br>08 8169 3900<br>gleahy@bps.sa.edu.au |

The School acknowledges and commits to adhere to the obligations contained within the Privacy Act and the Australian Privacy Principles (see Schedule 1 of the Privacy Act). In the event of a suspected or notified data breach, the following process will be followed.

### STAGE 1: DATA BREACH SUSPECTED OR NOTIFIED

Responsibility: All Staff

Time Frame: Immediately

If a Staff member discovers that a breach may have occurred (or is notified by a customer), they must immediately notify the Principal or the Business Manager by phone or email and document via email with as much detail as is known. This should include:

- Name of School/customer
- Name(s) of affected people, if known
- Evidence of breach - copies of any material which might constitute a breach

## STAGE 2: EVALUATION OF THE BREACH

The Business Manager will take responsibility for evaluation of the breach:

- Evaluate if a breach has occurred, or is likely to have occurred
- Document evaluation outcomes
- Determine if a breach has occurred.

### What constitutes a data breach?

- An eligible data breach occurs when three criteria are met:
    1. There is unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information that an entity holds
    2. This is likely to result in serious harm to one or more individuals
    3. The entity has not been able to prevent the likely risk of serious harm with remedial action
- 'Serious harm' can be psychological, emotional, physical, reputational or other forms of harm
- Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

### When should the Business Manager escalate a data breach?

The Business Manager may use discretion in deciding whether to escalate the breach to Step 3. Some data breaches may be comparatively minor and able to be dealt with easily without escalation. For example, it might be discovered that either a Staff member or a customer, as a result of human error, sent an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the sender can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue.

The Business Manager should use their discretion in determining whether a data breach or suspected data breach requires escalation. In making that determination, the Business Manager 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 the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in the School's processes or product?
- 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 it may be appropriate for the Business Manager to escalate the issue to Step 3. The Business Manager should have regard to CESA's Cyber Incident Response Plan.

### Business Manager to document minor breaches

If the Business Manager decides not to escalate a minor data breach or suspected data breach the Business Manager should create an incident report document, saved on the School's Learning Management System (SEQTA), containing:

- Description of the breach or suspected breach,
- Action taken by the Business Manager to address the breach or suspected breach,
- The outcome of that action, and
- The Business Manager's view that no further action is required.

## STAGE 3: IMPLEMENT DATA BREACH RESPONSE

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.

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

The Executive Team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

### 1. Contain the breach and do a preliminary assessment

a. Convene a meeting of the data breach response team

b. Immediately contain the breach i.e. if emails are still in queue, stop the queue and delete

c. Ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing the School to take appropriate corrective action

d. If the breach involves customer data, immediately establish contact with the ICT Systems Manager.

### 2. Evaluate the risks associated with the breach

a. Conduct an initial investigation and collect information about the breach promptly, including:

i. the date, time, duration and location of the breach

ii. the type of personal information involved in the breach

iii. how the breach was discovered and by whom

iv. the cause and extent of the breach

v. a list of the affected individuals or possible affected individuals

vi. the risk of serious harm to the affected individuals

vii. the risk of other harm

b. Determine whether the context of the information is important

c. Establish the cause and extent of the breach

d. Assess priorities and risks based on what is known

e. 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

f. Provide this information to the customer.

### 3. Consider breach notification

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

b. Discuss with customer and determine whether to notify affected individuals i.e. is there a real risk of serious harm to the affected individuals? 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

c. Consider whether others should be notified, including police/law enforcement, other agencies or organisations affected by the breach or where the School is contractually or otherwise required to notify specific parties

d. Determine whether notification to the Commissioner is required. If it is required, provide a copy of the notification to the customer.

**School contacts**

The School will request that all of its customers advise the appropriate contact person with whom the School will liaise in the event of a data breach.

**Who to notify**

Under the Act, the School must notify any individuals that are at likely risk of serious harm as a result of a data breach. The School must also notify the Commissioner.

There are 3 options for notification:

- notify all individuals whose personal information is involved in the eligible data breach
- notify only the individuals who are at likely risk of serious harm
- publish the notification and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm

The School will make a decision about the most appropriate option for notification on a case by case basis.

**Notification to the Commissioner**

The online form will be used to notify the Commissioner: https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

**4. Review the incident and take action to prevent future breaches**

a. Fully investigate the cause of the breach

b. Report to the School on outcomes and recommendations

   i. update security and Data Breach Response Plan, if necessary

   ii. make appropriate changes to policies and procedures, if necessary

   iii. revise staff training practices, if necessary

   iv. consider the option of an audit to ensure necessary outcomes are effected

c. Report to the customer a summary of the outcomes and recommendation.

## DEFINITIONS

***Customers***: includes Students, Staff, Parents, Family Members, Visitors, Volunteers, Old Scholars, Service Providers, the Catholic Church, and any other person for whom the School possesses data.

## RELATED DOCUMENTS/LINKS

1. Department for Education South Australia – www.education.sa.gov.au
2. Notifiable Data Breaches – Office of the Australian Information Commissioner: www.oaic.gov.au/privacy/notifiable-data-breaches/
3. CESA Cloud Computing Policy
4. CESA Cyber Incident Response Management Plan
5. CESA Information Security Policy
6. CESA Information Security Framework
7. CESA Information Security Classification Guideline

## IMPLEMENTATION

Responsibility for implementation, monitoring and review of the Data Breach Response Plan is vested in the following roles:

Business Manager

Principal

## REVIEW

Frequency: Every 2 years

Next review date: August 2022

## APPROVAL AUTHORITY / OWNER

Blackfriars Priory School