St Philip's Blackburn North

ST PHILIP'S DATA BREACH POLICY

VISION AND MISSION
Vision Statement

Modelling the teachings of Christ,
St Philip's School community aspires to be a place of welcome that provides many learning environments to meet the challenges of an ever-changing world.

Mission Statements
Because we believe that Christ is the central focus of our school and we are witnesses to him and his teachings we aim to:

- provide an atmosphere where all are made welcome, where they feel safe and have a sense of belonging
- provide a school environment that is positive and challenges all students to work to the best of their ability
- foster in all a realisation that they are responsible for their own learning
- develop a sense of justice by respecting the opinions and rights of others
- encourage all to be sensitive to others and respect their differences
- encourage all to use their physical environments in a respectful manner
- provide a learning environment that utilises the most effective and current approaches in education.

What is a Data Breach?
A data breach occurs when personal information that an organisation holds is subject to unauthorised access or disclosure, or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Organisations should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming ŏreasonably identifiableôas a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

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, as a result of inadequate identity verification procedures.

OAIC Data breach preparation and response. February 2018

Consequences of a data breach

The school needs to consider:

a. the kind of information

b. the sensitivity of the information

c. the extent to which the information is protected by security measures, e.g. encryption, passwords etc.

d. the kind of persons who have obtained, or could obtain, the information

e. the nature of the harm an individual could suffer e.g. physical, psychological, emotional or financial harm, or harm to reputation.

Data Collection:

St Philip's has a detailed Standard Collection notice that goes out to the school community each year. Collected data may include various types of personal information in both online and offline records – including photos of students, bank details, family information, contact details, and health information in the form of medical records or through counselling services.

Assessing a suspected breach:

A Data Breach Incident Reporting Form (Appendix A) should be completed by St Philip's Catholic Primary School staff in all instances of a data breach or suspected data breach. The form has two parts.
Part A is to be completed immediately by the person who discovers or suspects the breach. Details that need to be recorded include:

- the date, time, duration and location of the breach
- how the breach was discovered or is suspected
- description of the breach and the type of data involved
- the cause and extent of the breach
- any other staff members who either witnessed the event or were notified at the time of the incident

Part B is to be completed by the Principal and must include the following details:

- details of who is affected by the data breach and the estimated number of individuals affected
- a description of the immediate actions to be taken to contain the breach
- details of anyone else notified of the incident and, if so, how and when they were notified
- whether any evidence has been preserved
- if any other investigation is considered necessary
- if any steps have been undertaken to prevent the data breach from occurring again.

This assessment must be completed within 30 days of becoming aware of the suspected data breach.

References

Office of the Australian Information Commissioner.
Papers: Identifying eligible data breach; What to include in an eligible data breach statement

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

RELEVANT POLICIES

St Philip's Privacy Policy

REVIEW

Last reviewed: April 2018

Ratified by the Education Board: 1st May 2018

St Philip's Blackburn North

ST PHILIP'S DATA BREACH RESPONSE PLAN

This data breach response plan sets out procedures and clear lines of authority for St Philip's Catholic Primary School staff in the event that St Philip's 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. This response plan is intended to enable St Philip's to contain, assess and respond to data breaches in a timely fashion, 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 St Philip's to respond to a data breach.

ST PHILIP'S EXPERIENCES DATA BREACH/DATA BREACH SUSPECTED

Discovered by St Philip's staff member, or St Philip's otherwise alerted

What should the St Philip's staff member do?

- Immediately notify the Principal of the suspected data breach.
- Record, using the Data Breach Incident Reporting form, and advise your Principal of the time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

What should the Principal do?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (some breaches may be able to be dealt with at the Principal level).
- If so, immediately escalate to the Data Breach Response Team.

When should the Principal escalate a data breach to the OAIC Data Breach Response Team?

The Principal is to use discretion in deciding whether to escalate to the response team.

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (response team).
For example, a St Philipôs 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 recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue to the response team.
The Principal should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, the Principal 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 OAIC 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 óyesô, then it may be appropriate for the Principal to notify the response team.

The Data Response Team will consist of the Principal, Deputy Principal and the Digital Technologies Leader.

Minor Breaches Records Management

If the Principal decides not to escalate a minor data breach or suspected data breach to the response team for further action, the Principal should keep and store all documentation including:

- description of the breach or suspected breach
- action taken by the Principal to address the breach or suspected breach
- the outcome of that action, and
- the Principalôs view that no further action is required.

Data Breach Response Team Checklist

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.

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

- STEP 1: Contain the breach and do a preliminary assessment
- STEP 2: Evaluate the risks associated with the breach
- STEP 3: Notification
- STEP 4: Prevent future breaches

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

The response team should refer to the Data Breach preparation and response guide published by the Office of the Australian Information Commissioner (OAIC) in February 2018 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.

In reconsidering St Philipôs processes and procedures to reduce the risk of future breaches (Step 4) the response team should also refer to the OAICôs Guide to securing personal information. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for St Philipôs to take, in order to secure personal information, and considers actions that may be appropriate to help prevent further breaches following an investigation.

The following checklist is intended to guide the response team in the event of a data breach, and alert the response team to a range of considerations when responding to a data breach.

Records Management

Documents created by the response team should be saved and stored by the Principal at the school.

Step 1

Contain the breach and make a preliminary assessment

- The person who discovers the breach should immediately initiate a process of containment by taking whatever steps possible to immediately contain the breach. They must collect the necessary information, fill out part A of the Incident Reporting Form and notify the Principal.
- Convene a meeting of the data breach response team.
- Immediately contain breach:
- Ensure evidence is preserved that may be valuable in determining the cause of the breach.

Step 2

Evaluate the risks for individuals associated with the breach

- Conduct initial investigation and collect information about the breach promptly including: a) the date, time, duration and location of the breach, b) the type of personal information involved in the breach, c) how the breach was discovered and by whom, d) the cause and extent of the breach, e) a list of the affected individuals, or possible affected individuals , f) the risk of serious harm to the affected individuals and g) 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 to notify affected individuals - 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.
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach.
- Notify the Commissioner (OAIC) if necessary. Inform OAIC via their online form found at: https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB This should be done as soon as practicable after becoming aware of the eligible data breach.

Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Update security and response plan if necessary.
- Make appropriate changes to policies and procedures if necessary.
- Revise staff training practices if necessary.
- Consider the option of an audit to ensure necessary outcomes are effected.

Appendix A

ST PHILIP'S CATHOLIC PRIMARY SCHOOL REPORTING FORM

PART A – Information to be completed by staff reporting the incident	
Full Name	
Position:	
Contact Information:	
Details of the Incident	
Date, time, duration and location of the breach.	
How was the breach discovered?	
Description of the incident including others who may be affected.	
Cause of the breach (if known).	
Was any other staff member notified or witnessed the incident at the time?	
Signature: Date:	

ST PHILIP'S CATHOLIC PRIMARY SCHOOL REPORTING FORM

PART B – Information to be completed by the Data Custodian	
Full Name	
Position:	
Contact Information:	
Details of the Incident	
Who does the data breach affect? (e.g. staff, students, parents, general public, C.E.M., any other third party)	
Estimated number of individuals affected.	
Description of immediate actions taken to contain the breach.	
Was anyone else notified of the breach? (i.e. police, C.E.M., Office of the Information Commissioner etc.)	
Cause and estimated cost of the data breach (if known).	
Has evidence been preserved?	

Is further investigation considered necessary and how will this be undertaken?	
Have steps been taken to prevent the breach from occurring again?	
Signature:	Date: