St Geroge Preca Catholic Primary School	System Update: 01. 09. 2018	St George Preca Primary School learning through faith
Version 0.2	Date of Next Review: 01. 09. 2021	

Data Breach Procedure & Response Plan

Introduction:

St George Preca Primary School is committed to managing personal information in accordance with the Commonwealth Privacy Act 1988 (Cth), Australian Privacy Principles (APPs) and the school's Privacy Policy.

This document is designed to define the process the School will implement in the event of a data breach or where a suspected breach of data has occurred. A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, misuse or interference.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches Scheme (NDBS) that requires educational facilities and other organisations covered by the Act to notify any individual(s) likely to be at risk of 'serious harm' from a data breach. The NDBS also requires that the Office of the Australian Information Commissioner (OAIC) also be notified as the result of such an event.

Accordingly, St George Preca Primary School needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether the breach is likely to result in 'serious harm' and is eligible to be reported.

Adherence to this Procedure and Response Plan will ensure that the school can contain, assess and respond to data breaches promptly and mitigate potential harm to the person(s) affected.

The School will, from time to time, review and update this procedure to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

Definitions:

Data Breach: occurs where personal information is lost or subjected to unauthorised access, modification, disclosure, misuse or interference.

Eligible Data Breach: occurs where a data breach is likely to result in 'serious harm' to any individual(s) to who the information relates.

Notifiable Data Breach Scheme (NDBS 2018): An amendment to the Commonwealth Privacy Act 1988 (Cth) that requires school's & other organisations to notify an Eligible Data Breach to affected individual(s) and the Office of the Australian Information Commissioner (OAIC).

Personal information: is information or opinion, whether true or not, about a person whose identity is apparent, or can reasonably be ascertained, from the information or opinion – that is recorded in any form. For example, a person's name, address, phone number and date of birth (age). De-identified information about students can also be personal information.

Sensitive information: is information or opinion about a set of specific characteristics, including a person's racial or ethnic origin, political opinions or affiliations, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices; or criminal record. It also includes health information.

Serious Harm: May include physical, psychosocial, emotional, economic, financial harm or reputation damage resulting from any Data Breach.

Scope:

This procedure applies to all permanent, fixed term and casual employees at St George Preca Primary School, teaching & non-teaching. It also extends to contractors and volunteers (relevant Individuals) engaged to undertake work on behalf of the school.

Responsibilities:

School's Responsibility:
The school Principal, Members of the Leadership Team & the Parish Priest have a responsibility to:

- Ensure the security and privacy of any personal information collected by the school for educational and/or support services;
- Ensure all employees and other relevant individuals are aware of the school's Privacy Policy & Notifiable Data Breach Procedure;
- Act promptly in the event of a Data Breach (or suspected breach), and determine whether the breach is likely to result in 'serious harm' and in turn is eligible to be reported;
- Report any Eligible Data Breach to the Office of the Australian Information Commissioner (OAIC);
- Comply with legislative requirements.

Employee Responsibilities:

- Familiarise themselves with this policy and the school's Privacy Policy;
- Respect the confidentiality of personal information they obtain and the privacy of individual(s) associated with the school;
- Immediately report any Data Breach to the Principal, a Member of the Leadership Team or the Parish Priest;
- Work with the School to respond in the event of any Data Breach.

Processes where a Data Breach occurs or is suspected:

Alert:
Where a Data Breach is known to have occurred (or is suspected) the staff member(s) who identify this must bring it to the immediate attention of the School Principal, or in their absence, a Member of the School Leadership Team or the Parish Priest.

Information that must 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) Which directorate/faculty/institute is involved?;
f) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

The School maintains a Data Breach Process Form to assist in documenting the required information (Appendix A).

Assess & Determine the Potential Impact:
Once the Principal, Members of the Leadership Team & the Parish Priest (The Response Team) has been notified of the information above, consideration will be given as to whether a Data Breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. In determining this the Principal may seek advice from relevant Catholic Education Commission of Victoria (CECV) representative.

<u>Criteria for determining whether a Data Breach has occurred</u>:
The following aspects will be considered when determining whether a Data Breach has occurred:

a) Is personal information involved?;
b) Is the personal information of a sensitive nature? (Refer to Definitions);
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?

<u>Criteria for determining severity:</u>
The following criteria will be considered when determining the severity of any Data Breach:

a) The type and extent of personal information involved;
b) The number of individuals that 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 to the information;
e) Whether there is or could there be a real risk of ‘serious harm’ (physical, psychosocial, emotional, economic, financial harm or reputation) to the affected individual(s);

f) The possibility that there could be media or stakeholder attention as a result of the breach or suspect breach.

The School maintains a Data Breach Process Form to assist in assessing & determining the severity of any Data Breach (Appendix A).

'Non-Eligible' Data Breach

Upon review of the information provided, the Response Team will determine whether the breach is eligible for notification to the OAIC. Where it has been determined that a Data Breach has occurred; however, it is assessed not to cause 'serious harm' to the individual(s) affected, the breach will be managed at a school level by the Response Team.

To ensure an appropriate response to the identified breach the Response Team will:

- Immediately contain the breach;
- Immediately inform all members of the School Board and other key stake holders;
- Ensure that immediate corrective action is taken if this has not already occurred. This action may include but not be limited to informing all affected individuals of the breach;
- Retrieval or recovery of the personal information;
- Ceasing authorised access to the information;
- Shutting down or isolating the affected system;
- Prepare a briefing for Staff Members and the School Board.

Prepare a report containing the following:

- A description of the breach or suspected breach;
- The corrective action taken;
- Responsibilities & a timeframe for achieving the actions;
- The outcome of action taken;
- Processes to be implemented to prevent reoccurrence.

'Eligible' Data Breach - Notification

If there are reasonable grounds to deem the Data Breach to have the potential to cause 'serious harm' and hence be 'eligible of notification', the Response Team will immediately report this to the relevant Catholic Education Commission of Victoria (CECV) representative and prepare a Notifiable Data Breach Statement. (Appendix B).

The Notifiable Data Breach Statement must be finalised within 30 days and be submitted to the OAIC via its website. A Notifiable Data Breach Form may also be completed 'on-line' via the OAIC website.

The prescribed statement will be lodged by the Principal or a delegated representative.

Once the Notifiable Data Breach Statement has been lodged the Response Team conduct a thorough review of all aspects to:

- Determine remedial action/s required to reduce the likelihood of reoccurrence;

- » Ensure all relevant policies, procedures and processes are comprehensively reviewed and amended;
- » Prepare a report / briefing for Staff Members and the School Board;
- » Prepare a communication for the Parent Community outlining the breach, it's cause and action taken to contain, inform affected individual(s) and to prevent reoccurrence.

Consideration may be given to engaging a third party service to conduct a review of the school's Data Management and provide recommendations for improvement.

References:

Commonwealth Government 1988, *Privacy Act;*

Office of the Australian Information Commissioner (OAIC) 2014, Australian Privacy Principals;

Office of the Australian Information Commissioner (OAIC) 2018, Data Breach Notification Guide: A Guide to Handling Personal Information Security Breaches;

Office of the Australian Information Commissioner (OAIC) 2018, Data Breach Preparation & Response;

Office of the Australian Information Commissioner (OAIC) 2017, What to Include in an Eligible Data Breach Statement;

Victorian Government 2001, *Health Records Act*;

Data Breach Process Form

A Data Breach involves the loss of, unauthorised access to, or unauthorised disclosure of personal information.

This form will assist St George Preca Primary School Staff Members document the process where a Data Breach has occurred or is suspected to have occurred.

Data Breach Description:

St George Preca Primary School Staff Members are required to inform the Principal or a Member of the Leadership Team within 24 hours of identifying a Data Breach or suspected breach.

Data Breach Information	
Date of Breach:	
Anticipated Time of Breach:	
Description of Breach:	*Describe the type of personal information involved eg contact details, dates of birth.* ☐Financial Details ☐Contact Information ☐Health Information ☐Other Sensitive Information ☐ Other
Cause of Breach:	*If known, describe how the Data Breach was discovered.*
Which System(s) if Any Are Affected?:	*(SAS / nForma / Caremonkey / Skoolbag / Google Drive)*
Has Action Been Taken to Correct or Remedy The Breach?:	
Other Background Information:	

Reporting Staff Member:	
Date:	

Assessment & Determination of Potential Impact:

Member of St George Preca Primary School's Response Team including the Principal, Members of the Leadership Team and the Parish Priest must consider whether a Data Breach has, or is likely to have occurred and make a preliminary determination as to its severity.

Criteria for determining whether a Data Breach has occurred:	
Is Personal Information involved?:	Yes □ / No □
Is the Personal Information of a Sensitive Nature?:	*Sensitive Information: person's racial or ethnic origin, political opinions or affiliations, religious beliefs, philosophical beliefs, sexual preferences or practices; or criminal record.* Yes □ / No □
Has there been unauthorised access loss, disclosure of personal information where access to the information is likely to occur?:	Yes □ / No □

Criteria for determining the severity of the Data Breach:	
What type of Personal Information was involved & to what extent?:	*Names, address, phone numbers, dates of birth, academic records, student reports, financial information.*
Have multiple individuals been affected?:	Yes □ / No □ *If yes, provide further details*
Is the information protected by any security measures?:	Yes □ / No □ *If yes, provide further details*
Provide details on the person or kinds of people who now have access to the information:	
Determine whether there is, or could be a real risk of 'serious harm' to the affected individuals.	*Serious physical, psychosocial, emotional, economic, financial harm or reputation damage.*
Determine if there could be media or external stakeholder attention as a result of the breach or suspected breach.	*Media, Victoria Police,CECV, DEET, VRQA, Legal Representation.*
Other relevant Information:	

Where the Data Breach has been assessed to have the potential to cause 'serious harm', the school's <u>Notifiable Data Breach Statement</u> must be completed and submitted to the OAIC within 30 Days.

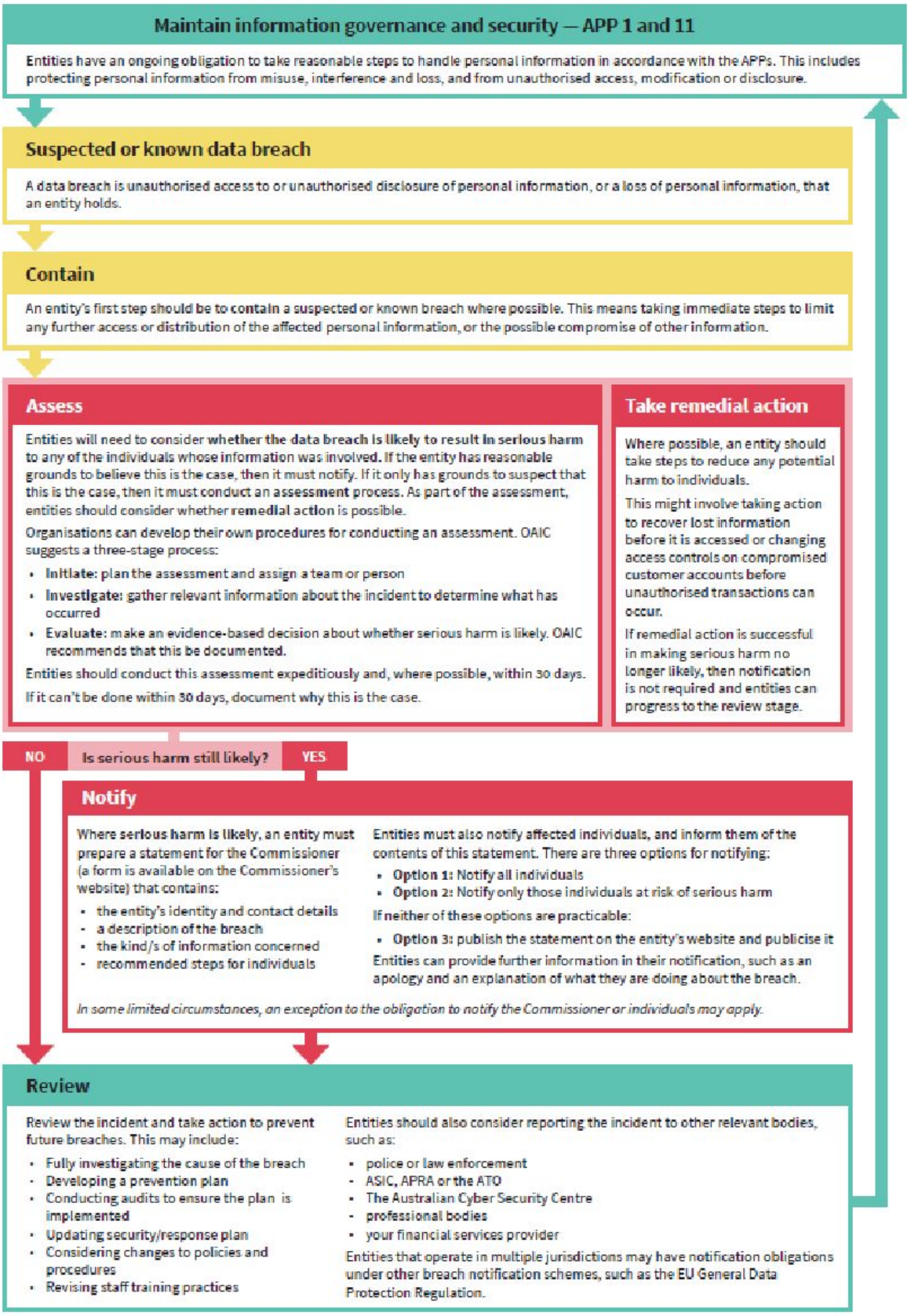
Notifiable Data Breach Statement

This statement must be submitted to the Office of the Australian Information Commissioner (OAIC) as soon as practicable after becoming aware of an 'Eligible Data Breach, and no later than 30 days, in accordance with the School's Data Breach Procedure and Response Plan.

Part 1	*Refers to requirements set out in section 26WK of the Privacy Amendment (Notifiable Data Breaches) Act 2017.*
Organisation Name:	
Contact Name:	
Contact Phone Number:	
Email Address:	
Description of the Notifiable Data Breach that the school has reasonable grounds to believe has happened.	
Types of Personal Information involved in the Data Breach.	☐Financial Details ☐Contact Information ☐Health Information ☐Other Sensitive Information ☐ Other:
Actions recommend that individuals take to reduce the risk that they experience 'serious harm' as a result of this data breach.	
Other affected entities:	Yes □ / No □ *If yes, provide further details*

Part 2	*The information that the school provides in Part Two of this form does not need to be included in the notification(s) to affected individuals. The School may request that it be held in confidence by the OAIC.*
Date of Breach:	
Date the Breach was Discovered:	
Primary cause of the Data Breach:	☐System Fault ☐Human Error ☐Malicious or Criminal Act ☐ Other:
A Description of how the Data Breach occurred:	
The anticipated number of individuals whose personal information is involved in the Data Breach	
A description of any action taken to assist individuals whose personal information was involved in the Data Breach.	
A description of any action taken by the school to prevent reoccurrence.	
How does the School intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach?	
When will this occur?	
List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to:	

Data Breach Response Process


Maintain information governance and security — APP 1 and 11
Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
Suspected or known data breach
A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.
Contain
An entity's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.
Assess
Entities will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an assessment process. As part of the assessment, entities should consider whether remedial action is possible.
Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:
Initiate: plan the assessment and assign a team or person
Investigate: gather relevant information about the incident to determine what has occurred
Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.
Entities should conduct this assessment expeditiously and, where possible, within 30 days.
If it can't be done within 30 days, document why this is the case.
Take remedial action
Where possible, an entity should take steps to reduce any potential harm to individuals.
This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.
If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.
NO
Is serious harm still likely?
YES
Notify
Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:
the entity's identity and contact details
a description of the breach
the kind/s of information concerned
recommended steps for individuals
Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:
Option 1: Notify all individuals
Option 2: Notify only those individuals at risk of serious harm
If neither of these options are practicable:
Option 3: publish the statement on the entity's website and publicise it
Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.
In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.
Review
Review the incident and take action to prevent future breaches. This may include:
Fully investigating the cause of the breach
Developing a prevention plan
Conducting audits to ensure the plan is implemented
Updating security/response plan
Considering changes to policies and procedures
Revising staff training practices
Entities should also consider reporting the incident to other relevant bodies, such as:
police or law enforcement
ASIC, APRA or the ATO
The Australian Cyber Security Centre
professional bodies
your financial services provider
Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.