Department: **Education**	Description: **Policy**
Administrative Area: **Risk Management and Compliance**	Type: **Mandatory**
Document Name: **Notifiable Data Breaches**	Issue Date: **22 September 2020**
Document ID: **SQS201.002.EDU**	Review Date: **Term 3 - 2022**

Noosa Christian College

Notifiable Data Breaches Policy

Purpose:	The purpose of this policy is to ensure that Seventh-day Adventist Schools (South Queensland) Limited is compliant with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988* (Privacy Act). Entities of Seventh-day Adventist Schools (South Queensland) Limited have data breach notification obligations when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach.	
Scope:	Students and employees, including full-time, part-time, permanent, fixed-term and casual employees, as well as contractors, volunteers and people undertaking work experience or vocational placements, where personal information is stored about these individuals	
References:	• Privacy Amendment (Notifiable Data Breaches) Act 2017 • Privacy Act 1988 (Cth) • SDAS(SQ)Ltd Privacy Policy (SQS130.003.ADM) • OAIC - Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Updated July 2019	
Status:	Approved	Supersedes: SQS201.001.ADM
Policy Owner:	Seventh-day Adventist Schools (South Queensland) Limited	
Authorised by:	Chief Executive Officer	Date of Authorisation: 22 September 2020
Approved by:	This policy has been ratified by the Board of Directors of Seventh-day Adventist Schools (South Queensland) Limited as the Notifiable Data Breaches Policy for Seventh-day Adventist Schools (South Queensland) Limited. **Pr Brett Townend** Board of Directors Chairperson — Date of Approval: 22/09/2020 **Pr Colin Renfrew** Board of Directors Secretary — Date of Approval: 22/09/2020	
Review Cycle:	Reviewed Biennially (every two years)	Next Review Date: Term 3 - 2022
Review Team:	Board of Directors, NSSAB, Chief Executive Officer, Project Officers	

Revised by	Section	Details of Changes
Steve Cowley (26 March 2018)	Whole document	As per BoD 'flying minute' of 26 February 2018: • document status changed from 'Draft' to 'Approved' • issue and approval dates changed to 26 February 2018 • names of BoD Chairperson and Secretary added • SDASSQ changed to SDAS(SQ)Ltd
Steve Cowley (6 April 2018)	Whole document	As per email from Jack Ryan 5 April 2018, changed Education Director and Chief Education Director titles to Chief Executive Officer

Department: **Education**	Description: **Policy**
Administrative Area: **Risk Management and Compliance**	Type: **Mandatory**
Document Name: **Notifiable Data Breaches**	Issue Date: **22 September 2020**
Document ID: **SQS201.002.EDU**	Review Date: **Term 3** - **2022**

Vanessa Woodman (7 September 2020)	Whole document	Updated references to the OAIC Data Breach Notification Guide to the *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Updated July 2019*

Overview

Seventh-day Adventist Schools (South Queensland) Limited is committed to ensuring that any personal information that it holds regarding students, parents, employees or volunteers will be stored securely in accordance with the guidelines from the Office of the Australian Information Commissioner and the existing personal information security obligations under the Australian *Privacy Act 1988* (Privacy Act).

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

Seventh-day Adventist Schools (South Queensland) Limited acknowledges the right of students, parents, employees and volunteers to reasonably expect that its entities will comply with the NDB with regards to investigation, containment, notification, assessment and review with regards to any identified data breaches. Further, it recognises that the NDB scheme strengthens the protections afforded to everyone's personal information and improves transparency in the way that organisations respond to serious data breaches.

Which Data Breaches Require Notification?

An 'eligible data breach', which triggers notification obligations, is a data breach that is *likely to result in serious harm* to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Examples of a data breach include when:

- a device containing personal information is lost or stolen;
- a database containing personal information is hacked;
- personal information is mistakenly provided to the wrong person.

For more information, refer to the following support documents from the Office of the Australian Information Commissioner (OAIC):

- *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) (July 2019)*
- *Identifying Eligible Data Breaches (December 2017)*

Assessing Suspected Data Breaches

Any entity of Seventh-day Adventist Schools (South Queensland) Limited that suspects an eligible data breach may have occurred must undertake reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected.

For more information, refer to the following support documents from the Office of the Australian Information Commissioner (OAIC):

- *Assessing a Suspected Data Breach (December 2017)*

How to Notify

When an entity of Seventh-day Adventist Schools (South Queensland) Limited is aware of reasonable grounds to believe an eligible data breach has occurred, they are obligated to promptly notify individuals at likely risk of serious harm. The Office of the Australian Information Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

The notification to affected individuals and the Commissioner must include the following information:

- the identify and contact details of the organisation;
- a description of the data breach;
- the kinds of information concerned; and,
- recommendations about steps individuals should take in response to the data breach.

For more information, refer to the following support documents from the Office of the Australian Information Commissioner (OAIC):

- *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – Part 4 - Notifying Individuals about an Eligible Data Breach (July 2019)*

Responsibilities

System Responsibilities

Seventh-day Adventist Schools (South Queensland) Limited acknowledges its responsibility to ensure the secure storage of personal information in accordance with *Privacy Act 1988* (Privacy Act) and the obligation to notify individuals as per the *Privacy Amendment (Notifiable Data Breaches) Act 2017* and will undertake the following steps as part of that system governance:

- Develop, implement, promote and act in accordance with the SDAS(SQ)Ltd Notifiable Data Breaches Policy (SQS201.002.EDU);
- Ensure that appropriate support is provided to all parties regarding training and procedures for keeping personal information safe and secure as per the *OAIC Guide to Securing Personal Information (June 2018)*;
- Receive from Seventh-day Adventist Schools (South Queensland) Limited entities reports of suspected or known data breaches;
- Take appropriate action to support the entity as they inform individuals of any eligible data breach;
- Complete the *Notifiable Data Breach Form* online to inform the Office of the Australian Information Commissioner on behalf of the entity.

School Responsibilities

The education entities of Seventh-day Adventist Schools (South Queensland) Limited acknowledges their responsibility to ensure the secure storage of personal information in accordance with *Privacy Act 1988* (Privacy Act) and the obligation to notify individuals as per the *Privacy Amendment (Notifiable Data Breaches) Act 2017* and will undertake the following steps as part of their compliance:

- Implement, promote and act in accordance with the SDAS(SQ)Ltd Notifiable Data Breaches Policy (SQS201.002.EDU);
- Appropriately communicate the SDAS(SQ)Ltd Notifiable Data Breaches Policy (SQS201.002.EDU) to students, parents and employees;
- Upon identification of a suspected or known data breach, assess the data breach in accordance with the process prescribed in *OIAC Identifying Eligible Data Breaches (December 2017)* and *OAIC Assessing a Suspected Data Breach (December 2017)*;
- Take steps to reduce any potential harm to individuals, such as recovering the lost information before it is accessed;
- As a result of the investigation, notify eligible data breaches to Seventh-day Adventist Schools (South Queensland) Limited through the Chief Executive Officer;
- With the support of the Chief Executive Officer, notify the individuals impacted by the breach of their data with reference to *OAIC Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) – Part 4 - Notifying Individuals about an Eligible Data Breach (July 2019)*
- Review the incident and take action to prevent further breaches.

Implementation

Seventh-day Adventist Schools (South Queensland) Limited is committed to raising awareness of the importance of maintaining personal information in a safe and secure manner at each of its educational entities, including by the development and implementation of this policy, related procedures and OAIC support documents, and via the clear support and promotion of the policy, procedures and support documents.

Seventh-day Adventist Schools (South Queensland) Limited is also committed to appropriately training relevant employees (especially senior staff) on how to take reasonable steps to handle personal information in accordance with the *Privacy Act 1988* (Privacy Act).

Seventh-day Adventist Schools (South Queensland) Limited will keep appropriate records of NDBs, will monitor NDBs and their resolution and will report on a high-level basis to the Board of Directors on NDB resolutions at each of its educational entities.

The individual educational entities of Seventh-day Adventist Schools (South Queensland) Limited will act to encourage students, parents and employees to contribute to a healthy school culture through the promotion of protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Compliance and Monitoring

Each school that is part of Seventh-day Adventist Schools (South Queensland) Limited will need to take reasonable steps to handle personal information in accordance with the *Australian Privacy Principles (APP)*:

- Consider whether to collect personal information – only collect personal information that is reasonably necessary to carry out your functions or activities. Over-collection can increase risks for the security of personal information;
- Privacy by design – you will be better placed to meet your personal information security obligations if you embed them early, as robust internal personal information handling practices, procedures and systems can assist you to embed good personal information handling practices and respond effectively in the event a privacy breach occurs;
- Assessing the risks – conduct a privacy impact assessment, an information security risk assessment and reviews of your personal information security controls so that you are aware of the variety of security risks you face, including threats and vulnerabilities, along with the possible impacts before designing and implementing your personal information security framework;
- Take appropriate steps and put into place strategies to protect personal information – consider what appropriate security measures are required to protect the personal information with regards to all of the entity's acts and practices;
- Destroy or de-identify personal information – take reasonable steps to destroy or de-identify the personal information that was once held but is no longer needed for any purpose.

For more information on compliance and monitoring, refer to *OAIC Guide to Securing Personal Information (June 2018)*.

Additional Resources from OAIC

- *OAIC - Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Updated July 2019*

Appendix A

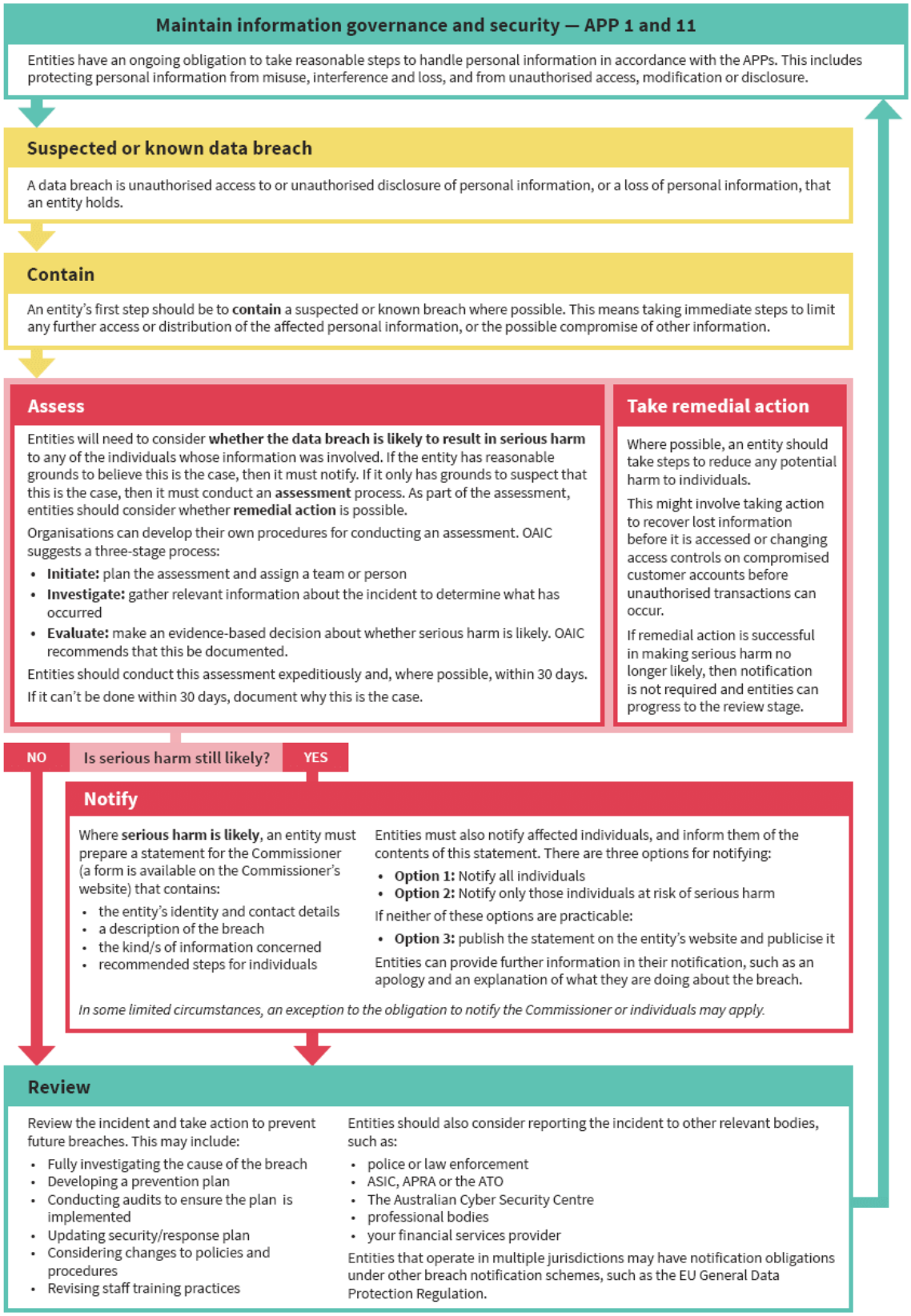
- *OAIC - Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Updated July 2019 – PART 3*

Appendix B

https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

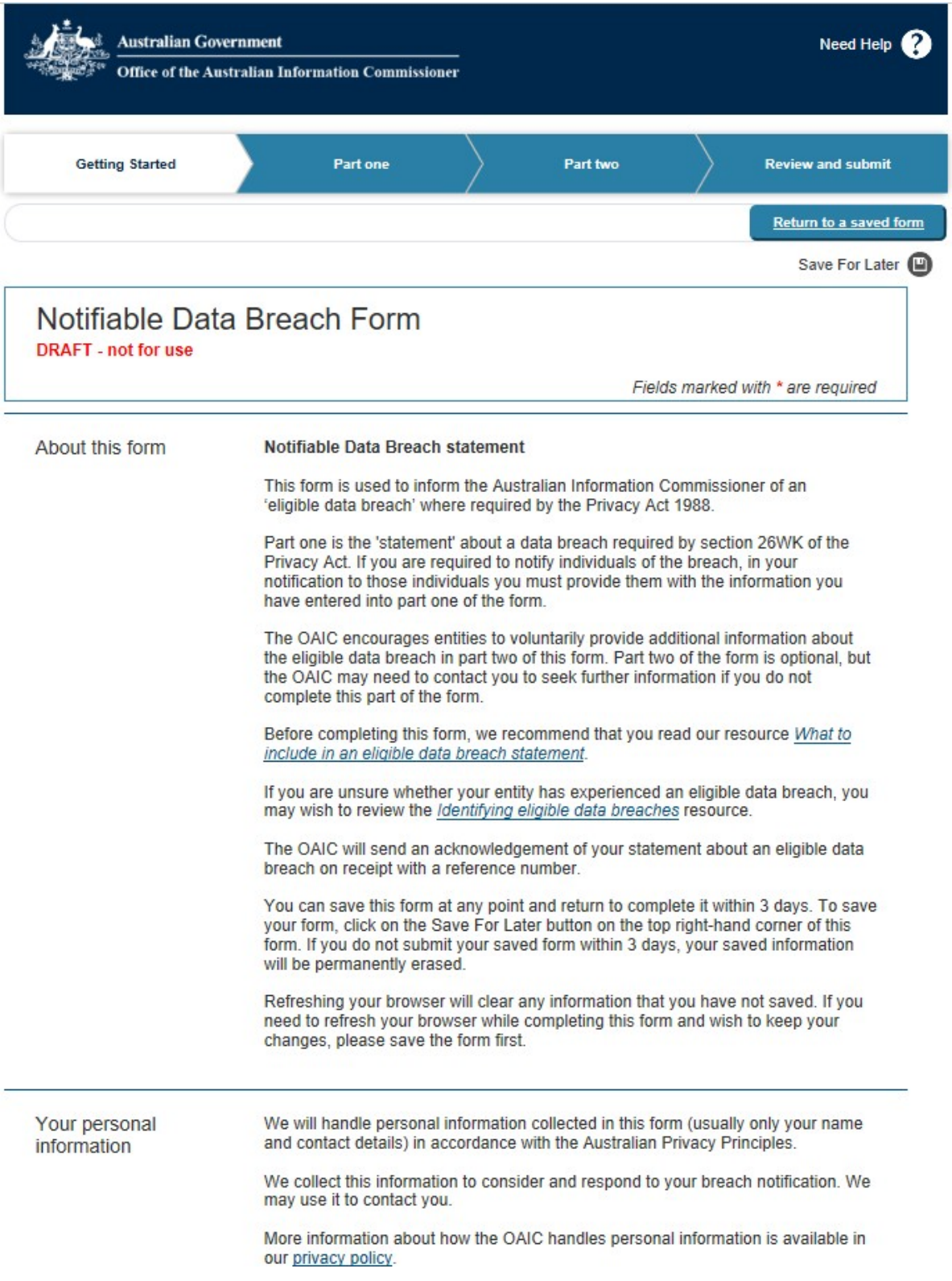
Data Breach Response Summary

Appendix A



Notifiable Data Breach Form (Online)

Appendix B



Australian Government
Office of the Australian Information Commissioner

Need Help

Getting Started | Part one | Part two | Review and submit

Return to a saved form

Save For Later

Notifiable Data Breach Form

DRAFT - not for use

*Fields marked with * are required*

About this form

Notifiable Data Breach statement

This form is used to inform the Australian Information Commissioner of an 'eligible data breach' where required by the Privacy Act 1988.

Part one is the 'statement' about a data breach required by section 26WK of the Privacy Act. If you are required to notify individuals of the breach, in your notification to those individuals you must provide them with the information you have entered into part one of the form.

The OAIC encourages entities to voluntarily provide additional information about the eligible data breach in part two of this form. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form.

Before completing this form, we recommend that you read our resource *What to include in an eligible data breach statement*.

If you are unsure whether your entity has experienced an eligible data breach, you may wish to review the *Identifying eligible data breaches* resource.

The OAIC will send an acknowledgement of your statement about an eligible data breach on receipt with a reference number.

You can save this form at any point and return to complete it within 3 days. To save your form, click on the Save For Later button on the top right-hand corner of this form. If you do not submit your saved form within 3 days, your saved information will be permanently erased.

Refreshing your browser will clear any information that you have not saved. If you need to refresh your browser while completing this form and wish to keep your changes, please save the form first.

Your personal information

We will handle personal information collected in this form (usually only your name and contact details) in accordance with the Australian Privacy Principles.

We collect this information to consider and respond to your breach notification. We may use it to contact you.

More information about how the OAIC handles personal information is available in our privacy policy.

Australian Government
Office of the Australian Information Commissioner

Need Help

Getting Started | Part one | Part two | Review and submit

Save For Later

Part one - Statement about an eligible data breach

Notifiable data breach form

*Fields marked with * are required*

About part one

The information that you provide to the OAIC in part one of this form must also be included in your notification to individuals (if notification is required).

Organisation/agency details

You must complete this section

Organisation/agency name

Phone

Email

Address Line 1

Address Line 2

Suburb

State

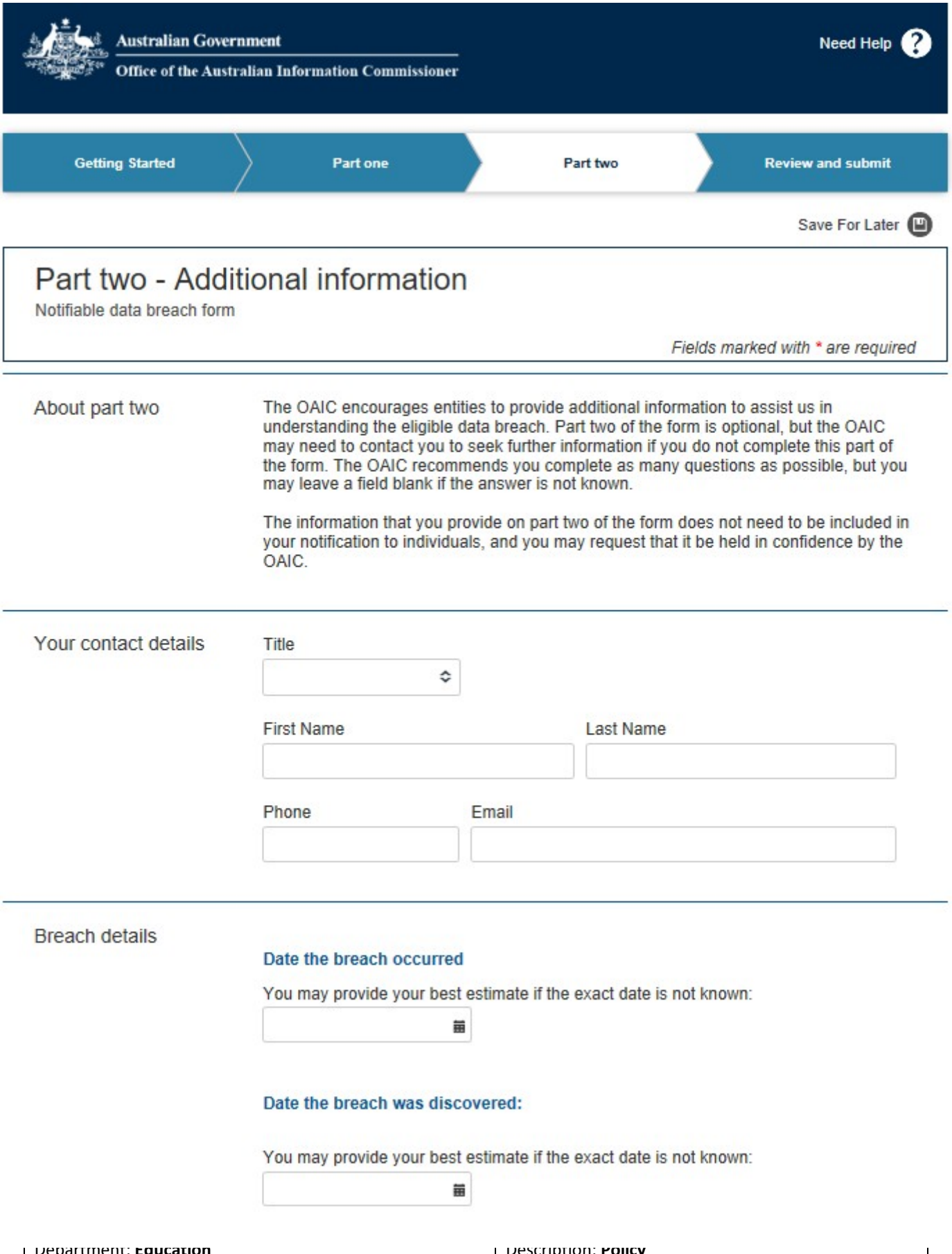
Postcode

Other contact details

Description of the eligible data breach

You must complete this section

A description of the eligible data breach:


Australian Government
Office of the Australian Information Commissioner
Need Help
Getting Started
Part one
Part two
Review and submit
Save For Later
Part two - Additional information
Notifiable data breach form
Fields marked with * are required
About part two
The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form. The OAIC recommends you complete as many questions as possible, but you may leave a field blank if the answer is not known.
The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.
Your contact details
Title
First Name
Last Name
Phone
Email
Breach details
Date the breach occurred
You may provide your best estimate if the exact date is not known:
Date the breach was discovered:
You may provide your best estimate if the exact date is not known:

Information involved in the data breach

You must complete this section

Kind or kinds of personal information involved in the data breach:

In addition, please select any categories that apply:

- ☐ Financial details
- ☐ Tax File Number (TFN)
- ☐ Identity information (e.g. Centrelink Reference Number, passport number, driver license number)
- ☐ Contact information (e.g. home address, phone number, email address)
- ☐ Health information
- ☐ Other sensitive information (e.g. sexual orientation, political or religious views)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach:

Other entities affected

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation/agency affected?

- ○ Yes
- ○ No

Go Back | Continue

Primary cause of the data breach:

- ○ Malicious or criminal attack
- ○ System fault
- ○ Human error

Description of how the data breach occurred

Number of individuals whose personal information is involved in the data breach

- ○ 1
- ○ 2 – 10
- ○ 11 - 100
- ○ 101 - 1,000
- ○ 10,001 - 100,000
- ○ 100,001 - 1,000,000
- ○ 1,000,001 - 10,000,000
- ○ 10,000,001 or more

Exact number of individuals whose personal information is involved in the data breach

Please provide your best estimate:

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach

Description of any action you have taken, or you are intending to take, to prevent reoccurrence

How do you 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? If you do not intend to notify individuals because of an exception under s 26WN or s 26WP, please provide your reasons for relying on the relevant exception.

List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to:

Additional information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?

You can provide additional information below, or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to enquiries@oaic.gov.au.

Comments

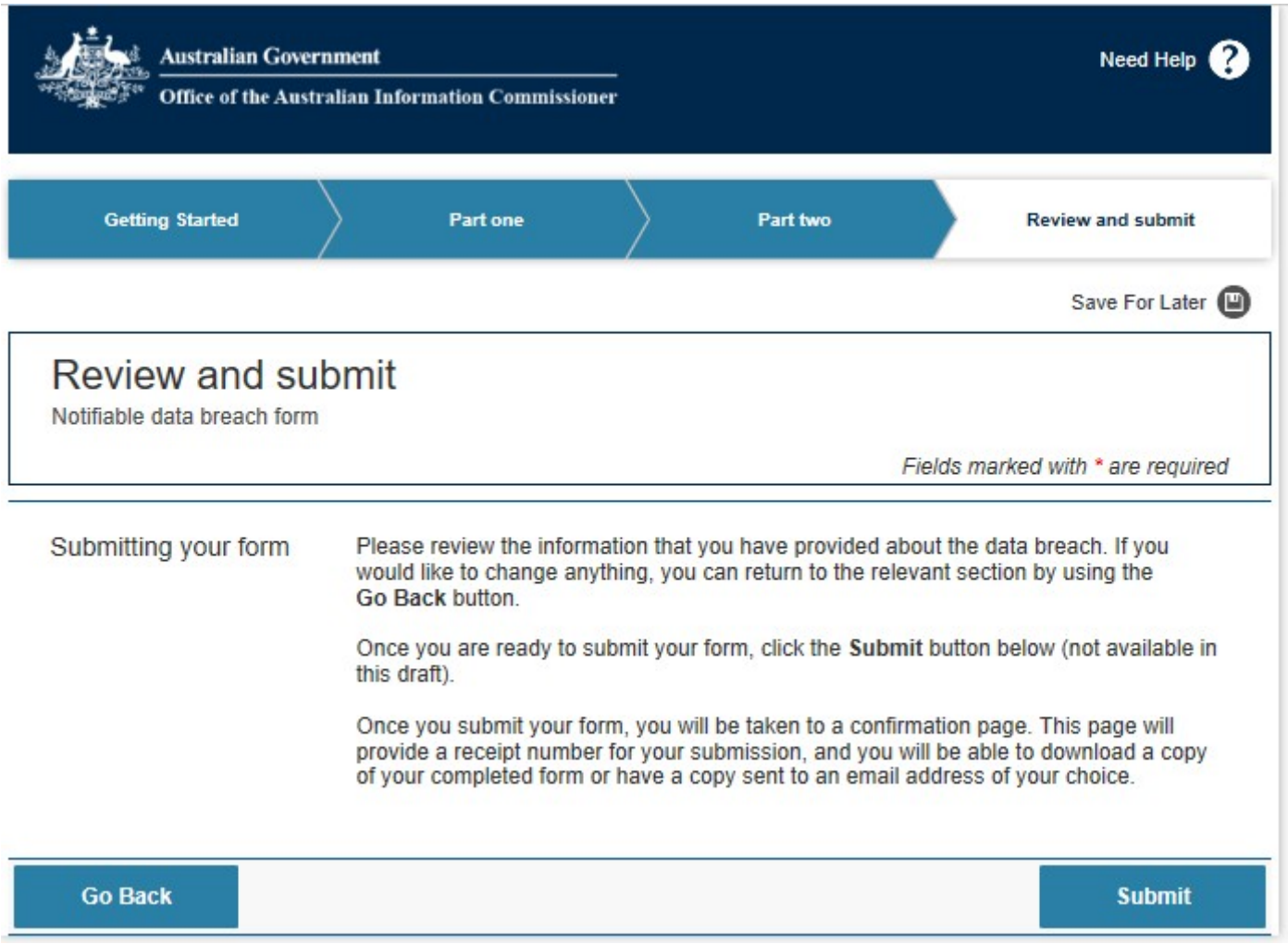
Attachments

Click to Upload

I request that the information provided in part two of this form is held by the OAIC in confidence.

The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

Go Back **Continue**


Australian Government
Office of the Australian Information Commissioner
Need Help
Getting Started
Part one
Part two
Review and submit
Save For Later
Review and submit
Notifiable data breach form
Fields marked with * are required
Submitting your form
Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section by using the Go Back button.
Once you are ready to submit your form, click the Submit button below (not available in this draft).
Once you submit your form, you will be taken to a confirmation page. This page will provide a receipt number for your submission, and you will be able to download a copy of your completed form or have a copy sent to an email address of your choice.
Go Back
Submit