

AUGUSTINIANS



PROVINCE OF OUR MOTHER OF GOOD COUNSEL AUSTRALASIA

GENERAL PRIVACY POLICY

INTRODUCTION

1. This policy applies to applications to enter the Province of the Order of St Augustine in Australasia, to subsequent membership, and to information kept by the Province.
2. The Province has adopted the National Privacy Principles as its code of practice.

PERSONAL INFORMATION COLLECTED

3. The personal information collected on applicants and members of the Province is necessary for the functions and activities of the Province. It may comprise: the applicant's or member's name, address, occupation, age, contact details, family background, parents' present marital status and contact details, next of kin details, place of birth, country of citizenship, religious details and practices, health information including physical and psychological details and criminal charges, private health insurance details, Centrelink details, medical and Health Card numbers, bank account details, formation assessments, academic records, and general correspondence. This list is not exhaustive.
4. When information is obtained from a third party, reasonable steps will be taken to ensure the subject is made aware of the matters.
5. Applicants will be asked to sign a release form regarding medical and psychological history and assessment.

THE PURPOSE FOR HOLDING PERSONAL INFORMATION

6. The activities and functions of the Province necessitate the holding of personal information on applicants and members.
7. The reason for obtaining and storing this information is to understand better the needs, requirements and suitability of applicants and members.

USE AND DISCLOSURE OF PERSONAL INFORMATION

8. Personal information collected may be accessible by superiors and formators on the basis that it will remain confidential. It is accessible by a limited and defined number of people.
9. If an applicant or member applies to another religious institute or diocese, the Province is required by Canon Law to provide a report to such institute or diocese.
10. Personal information will not be released to third parties unless:
 - The applicant or member has consented to the disclosure;
 - The Province is required or authorized by law to do so;
 - The Province considers itself to have been released from their duty of confidentiality so that there is no alternative but to respond publicly.
11. If personal information is sent overseas it will be subject to the same systems of access and storage as apply in Australia.

PERSONAL INFORMATION: QUALITY

12. This Privacy Policy is premised on ensuring the information held by the Province is accurate, complete and up-to-date.
13. If any of the information provided has changed or is considered incorrect, the person concerned should contact the Privacy Officer.

PERSONAL INFORMATION: SECURITY

14. The Provincial Office and the houses of the Province have secure storage units with defined limited access.
15. This includes physical security, computer and network security, communications security and personnel security.
16. The purpose is to protect personal information from misuse, loss, unauthorized access, modification or disclosure.

ACCESS TO PERSONAL INFORMATION

17. The Province will provide access to an applicant's or member's personal information that has been compiled after 21 December 2001.
18. Where the information has been compiled prior to 21 December 2001 it will be provided if it has been used or disclosed after 21 December 2001.
19. A request to access information should be made in writing to the Privacy Officer, care of the Provincial Office.
20. If a request is declined, the person making the request will be given the reason.

DESTROYING PERSONAL INFORMATION

21. Personal information will be retained for an appropriate period as determined by government legislation, and thereafter will be destroyed by a secure means. (Also refer to 'Other Information – Safeguarding' no 24).

OTHER INFORMATION

22. From time to time, the Province keeps other information, including, for example, data banks of names, addresses and contact details of donors, clients and subscribers to occasional publications.
23. Such information will not be shared with other parties, but will remain confidential.

OTHER INFORMATION - SAFEGUARDING

24. All critical information related to safeguarding, (e.g. background checks, complaints and incidents) including the results of decisions and actions taken will be held for 50 years and in accordance with any record keeping requirements by law. All files are retained in the Provincial Administration Office in a secure manner with access restricted.
25. Records will adhere to the principles of good record keeping, including:
 - a) ensuring records are accurate and complete and adequately detail all incidents, complaints, responses and decisions;
 - b) records are created at the time of, or as soon as practicable following, an incident, complaint, response or decision;
 - c) records are titled, organised and filed logically;
 - d) a master copy of each record is formally maintained to ensure duplicate records or multiple copies of the same record are kept to a minimum;
 - e) sharing or distribution of information and/or records is restricted to nominated personnel and is conducted in accordance with relevant legislative and statutory requirements; and

f) individuals' rights to access, amend or annotate records about themselves are recognised to the fullest extent.

FUNDRAISING PRIVACY POLICY

We will ensure:

26.1 When collecting personal information from donors, volunteers, clients and others, and intending to use that information for fundraising purposes, we notify them about that from our initial contact.

26.2 If we have not notified a person that their personal information might be used for fundraising purposes, we do not use it for those purposes unless:

- we first obtain consent, or
- an exception applies (for example, for non-sensitive personal information, that the fundraising purpose is related to the primary purpose and the person would reasonably expect you to use the information in that way).

26.3 if we share your donor lists with other organisations, we will ensure the person(s) are advised prior or upon initial contact.

26.4 We will always offer donors who support fundraising campaigns a choice about receiving information on non-fundraising activities or new campaigns at the start, and provide an opt out option in all fundraising communications.

We will allow staff access to client information on a 'need to know' basis. For example, ensure that those involved in soliciting donor memberships do not have routine access to personal information that may be kept on client databases, and have checks and balances in place to protect the security of personal information.

It is also important to familiarise with the fundraising laws applicable in each state and territory where your not-for-profit organisation is conducting fundraising activities.

COMPLAINTS PROCEDURE

27. The process allows an individual to:

- Apply first to the Privacy Officer who will deal with the complaint;
- Appeal the matter to the Privacy Committee of the Province, and finally to the Privacy Commissioner.

CHANGES TO THE PRIVACY POLICY

28. The Provincial and Council may make changes as may be necessary to this Privacy Policy at any time. Such changes will be publicised to the Province.



Order of St Augustine Cyber Privacy Policy

This policy sets out how OSA manages privacy obligations and reflects the 13 Australian Privacy Principles (APPs) from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), which amends the Privacy Act 1988 (Cth).

1. Background Information

2. Policy Statement

3. Policy Purpose

4. Application of Policy

5. Privacy Principles

6. Roles and Responsibilities

7. Policy Review

8. Further Assistance

9. Glossary of Terms

1. **Background Information**

1.1 Order of St Augustine (**OSA**) is subject to the Commonwealth *Privacy Act* 1988 (**Act**). The *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 which commenced in March 2014 made significant changes to the Act. This Policy complies with the new requirements imposed by the Act.

2. **Policy Statement**

2.1 OSA is committed to managing personal information in an open and transparent way. OSA is a registered company and is subject to the requirements of the Act. It adheres to the Australian Privacy Principles (**APPs**) set out in Schedule 1 to the Act.

3. Policy Purpose

3.1 This Policy sets out how OSA collects, holds, uses and discloses personal information including sensitive information.

4. Application of Policy

4.1 Subject to clause 4.2, this Policy applies to all personal information and sensitive information collected and held by OSA.

4.2 Despite clause 4.1, any act that has been done or practice engaged in by OSA which is directly related to:

- a current or former employment relationship between OSA and an individual, and
- a current or historical employee record held by OSA relating to an individual

are exempt from this Policy in accordance with the Act and the APPs.

4.3 Employee records are governed by the provisions of OSA's *Employee Records Privacy Policy*.

5. Privacy Principles

5.1 Personal information collected and held by OSA

OSA collects personal information for the purposes of OSA's functions and activities. It collects personal information about staff, members of the province, financial donors and other individuals who have dealings with OSA for administrative need, to conduct its business, for legislative compliance or for research purposes.

The information may include residence and contact details, date of birth, details of next of kin, identifying information, including photographs, records of injuries, criminal checks, qualifications and financial information.

Some of the personal information that OSA collects and holds is sensitive information. OSA only collects sensitive information where it is necessary for the purpose for which it is being collected and with the individual's consent unless the collection is required or authorised by law.

5.2 How OSA collects and holds personal information

OSA collects and holds information from a number of sources. Where reasonably possible, OSA will only collect information from the individual to whom it relates. Frequently this will be collected through official OSA administrative processes but it may also be collected from email, letters or other forms of communication.

OSA also holds personal information about individuals that it generates in the course of its operational activities, such as fundraising activities, newsletter subscribers, financial donors and friends of the Order of St Augustine.

Personal information is held in both paper and electronic form, including databases.

When an individual visits the OSA website, log files (“cookies”) are created by the web server that contain certain information including the Internet Protocol (IP) address of the visitor, the previous site visited, the time and date of access and pages visited and downloaded. Cookies allow a website, such as the OSA website, to temporarily store information on an individual’s machine for later use. OSA’s website uses cookies to identify unique visitors to the site.

In order to improve OSA’s services and assist the user, OSA may store information about users of its website to create a digital profile and provide them with information specific to them.

OSA also uses Web Analytics to obtain statistics about how its website is accessed. Web Analytics relies upon cookies to gather information for the purpose of providing statistical reports to OSA. The information generated by the cookie about an individual’s use of the OSA website is transmitted to and stored by Web Analytic service providers on servers located within and outside Australia, but it does not include any personally identifying information.

Individual users generally have the option of accepting or rejecting cookies by adjusting the settings in their web browsers. However, rejecting cookies may impact upon the functionality of the OSA website.

The OSA website may contain links to other websites. OSA cannot control the privacy controls of third party websites. Third party sites are not subject to OSA’s Privacy Policy or Procedures.

5.3 Notification of collection of personal information

When OSA collects personal information it will advise the individual why it is collecting that information and how it uses it, whether the collection of the information is required or authorised by law and the consequences for the individual if the personal information is not collected. It will also provide information about OSA’s Privacy Policy and about the right of individuals to access and correct personal information. If OSA collects personal information in circumstances where the individual may not be aware of the collection it will seek to advise the individual of the collection.

5.4 The purposes for which OSA collects, holds, uses and discloses personal information

OSA collects and uses personal information for a variety of different purposes relating to its functions and activities including:

- Fundraising activities
- Newsletter generation and distribution
- Community engagement
- Government reporting
- Commercial application of its intellectual property and professional expertise
- Undertaking staff and student recruitment activities

- Undertaking research
- Handling complaints
- Conducting its business and improving the way in which it conducts its business
- Purposes directly related to the above.

5.5 Use or disclosure for secondary purposes

OSA does not use or disclose personal information for purposes other than the purpose for which it was collected (**the primary purpose**) unless:

5.5.1 the individual has consented to a secondary use or disclosure, or

5.5.2 the secondary use or disclosure is related to the primary purpose (in the case of personal information that is not sensitive information) or is *directly* related to the primary purpose (in the case of sensitive information), or

5.5.3 it is otherwise required or authorised by or under an Australian law or a court/tribunal order, or

5.5.4 a permitted general situation exists (as described in clause 9 of this policy), or

5.5.5 OSA reasonably believes that it is necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

In ordinary circumstances, any disclosure of personal information for a secondary purpose under scenarios 5.5.3, 5.5.4 and 5.5.5 must be approved by the Privacy Officer.

5.6 Security

OSA applies both physical and information and communications technology (ICT) security systems to protect personal information.

In relation to electronic records, personal information is collected via OSA's systems including web-based systems. OSA has put in place measures to protect against loss, misuse and alteration of electronic information. Where necessary, OSA also uses encryption technology to protect certain information and transactions.

5.7 Remaining anonymous or using a pseudonym

OSA understands that anonymity is an important aspect of privacy and that in some circumstances some people may prefer to use a pseudonym when dealing with OSA. People have the right to remain anonymous or to use a pseudonym when dealing with OSA.

5.8 Unsolicited personal information

When OSA receives unsolicited personal information it will assess whether it is personal information that it could legally collect. If it is, it will treat it according to the APPs. If it is not, it will, if lawful to do so, destroy or de-identify it as soon as practicable.

5.9 Direct marketing

OSA will only use personal information for direct marketing with the individual's consent or when authorised by law.

5.10 Destruction of information that does not need to be retained

When OSA no longer needs to retain personal information, and is lawfully able to do so, it will destroy or de-identify that information. (Please also refer to 'General Privacy Policy' no 24).

5.11 How an individual may access personal information about the individual that is held by OSA

Subject to clause 4.2, anyone has a right under the Act to access personal information that OSA holds about them. Access to personal information is governed by the *Access to and Correction of Personal Information Procedure*.

5.12 How an individual may seek the correction of personal information about the individual that is held by OSA

Subject to clause 4.2, anyone has a right under the Act to request corrections to any personal information that OSA holds about them if they think that the information is inaccurate, out of date, incomplete, irrelevant or misleading. Correction of personal information is governed by the Access Procedure.

5.13 How an individual may complain about a breach of the Australian Privacy Principles by OSA

Subject to clause 4.2, anyone may complain about a breach of an APP by OSA. Complaints should be made in to the Prior Provincial or Province Secretary via mail, PO Box 7278 Warringah Mall, Brookvale 2100, via phone, 02 9938 0200 or via email, osaadmin@bigpond.com.

5.14 How OSA will deal with complaints about breaches of the Australian Privacy Principles

OSA will deal with complaints about breaches of the APPs in accordance with the suggested complaints procedures by the Act.

5.15 How OSA will manage an actual or suspected data breach under this policy

OSA will manage the process of dealing with an actual or suspected breach in accordance with the *Data Breach Procedure of the Act*.

5.17 Disclosure of personal information to third parties

OSA may disclose information to third parties to

- provide services

- for purposes of research to improve its operations and services
- promote its activities
- if permitted or required by law, or
- otherwise with the consent of the individual.

Where OSA discloses personal information to third parties it will require restrictions on the collection and use of personal information equivalent to those required of OSA by the *Privacy Act 1988*.

6. Roles and Responsibilities

6.1 Approval Authority

The Provincial Council is the Approval Authority for this Policy.

6.2 Governing Authority

The Prior Provincial is the Governing Authority for this Policy.

6.3 Responsible Officer

- Fr David Austin OSA is the Responsible Officer for this Policy.

6.4 Other Roles

- Fr David Austin OSA is the OSA Privacy Officer.

7. Policy Review

7.1 Review

OSA will review this Policy and the Procedure regularly. It may amend the Policy and Procedure from time to time to ensure their currency with respect to relevant legislation and Order Policy and Procedures and to improve the general effectiveness and operation of the Policy and Procedures.

In line with the Order's *Policy on Policy Development* and *Policy Development Procedure*, this Policy is scheduled for review every five (5) years or sooner in the event that the Approval Authority or Governing Authority determine that a review is warranted. The Policy and Procedures will initially be reviewed one (1) year following the Effective Date.

7.2 Revisions made to this document

<u>Date</u>	<u>Major/Minro Revision</u>	<u>Description of Revision</u>
Nov '18	Major	Policy submission and approval by Prov Council
Oct '20	Minor	Include 'Other Information – Safeguarding' – approved by Prov Council – Oct '20.

Further Assistance

8.1 Alternative formats

Access to this Policy in alternative formats (e.g. hard copy) is available through the Privacy Officer whose contact details are listed under “Contact details” at the end of this Policy.

8.2 Contact details

Contact for all matters related to privacy should be directed as follows:

Professional Standards Co-ordinator/Privacy Officer, Fr David Austin OSA

E: dave.austin@osa.org.au

T: 02 9905 3022

P: PO Box 7278 Warringah Mall, Brookvale 2100

9. Glossary of Terms

Access Procedure means the *Access to and Correction of Personal Information Procedure* promulgated under this Policy.

Act means the *Privacy Act 1988 (Cth)*.

Australian Privacy Principles (APPs) means the 13 APPs set out in Schedule 1 of the Act.

9. Terms & Notes

Data breach means the loss, unauthorised access to, or disclosure of, personal information.

Employee record means a record of confidential personal information relating to the employment of a staff member. The employee record comprises information about employment, including health, recruitment and selection, terms and conditions of employment, performance, discipline, and resignation. Employee records are exempt from the provisions of the Act.

Inquiries and Complaints Procedure means the *Privacy Inquiries and Complaints Procedure* promulgated under this Policy.

Loss means accidental or inadvertent loss of personal information likely to result in unauthorised access or disclosure. For example, an employee leaves a copy of a document or a device on public transport. If data can be deleted remotely or is encrypted it will not constitute an NDB.

Notifiable Data Breach (NDB) is a data breach that is likely to result in serious harm to any of the individuals to whom the personal information relates. A NDB occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. In such circumstances, OSA must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as required under the Privacy Amendment (Notifiable Data Breaches) Act 2017

Permitted general situation has the same meaning as provided for in section 16A of the Act and referred to in APP 6.2(c). The permitted general situations are: lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety; taking appropriate action in relation to suspected unlawful activity or serious misconduct; locating a person reported as missing; asserting a legal or equitable claim; conducting an alternative dispute resolution process.

Personal information means information or an opinion in any form about an identifiable individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not.

Privacy Officer means the person appointed by OSA from time-to-time to manage and coordinate OSA's compliance with the Policy and the Procedures at the direction of the Privacy Officer.

Privacy Officer means the person appointed by OSA from time-to-time to manage all inquiries and complaints arising under this Policy. The Privacy Officer may delegate the management of any or all of the inquiries and complaints arising under this Policy to the Privacy Officer.

Sensitive information means information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record, or health information, genetic information or biometric information.

Serious harm is determined based on the following list of relevant matters as provided for in section 26WG of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*:

- the kind or kinds of information;

- the sensitivity of the information;
- whether the information is protected by one or more security measures;
- if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
- if a security technology or methodology:
 - was used in relation to the information; and
 - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information; the likelihood that the persons, or the kinds of persons, who:
 - have obtained, or who could obtain, the information; and
 - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
 - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology; the nature of the harm; any other relevant matters.

Unauthorised access means personal information accessed by someone who is not permitted to have access. This could include an employee of the entity, a contractor or external third party (such as hacking, device theft or data theft).

Unauthorised disclosure means where an entity releases/makes visible the information outside the entity in a way not permitted by the Privacy Act. For example, an employee accidentally publishes a confidential data file containing personal information on the internet.

Web Analytics means the measurement collection, analysis and reporting of web data for the purpose of understanding and optimising web usage.



Order of St Augustine Notifiable Data Breach Policy (NDB)

1. Policy

This Procedure is governed by the Order of St Augustine (OSA) *Privacy Policy*.

2. Introduction

OSA is committed to managing personal information in accordance with the *Privacy Act 1988 (Cth)* (the Act) and the OSA Privacy Policy.

This document sets out the processes to be followed by OSA staff in the event that OSA experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

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, OSA 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.

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

This Procedure and Response Plan has been created based on the following guides:

- The Office of the Australian Information Commissioner's "*Guide to developing a data breach response plan*"
- The Office of the Australian Information Commissioner's "*Data breach notification guide: a guide to handling personal information security breaches*"
- NDB Act of 2018
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

This document should be read in conjunction with OSA's *Privacy Policy*.

3. Process where a breach occurs or is suspected

3.1 Alert

Where a privacy data breach is known to have occurred (or is suspected) any member of OSA staff who becomes aware of this must, within 24 hours, alert a Member of the Province Administration 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. Where the breach occurred (location, device being used)
- c. Description of the breach (type of personal information involved)
- d. Cause of the breach (if known) otherwise how it was discovered
- e. Which system(s) if any are affected?
- f. Whether corrective action has occurred to remedy the breach (or suspected breach)

3.2 Assess and determine the potential impact

Once notified of the information above, the Member of the Province Administration must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The Privacy Coordinator should be contacted for advice.

3.2.1 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?

For the purposes of this assessment the following terms are defined in section 9 of the *Privacy Policy*: personal information, sensitive information, unauthorised access, unauthorised disclosure and loss.

3.2.2 Criteria for determining severity

- a. The type and extent of personal information involved
- b. Whether one or 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 there 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 suspect breach

In relation to 3.2.2(e) above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in section 9 of the *Privacy Policy* and section 26WG of the NDB Act.

Having considered the matters in 3.2.1 and 3.2.2, the Member of the Province Administration must notify the Privacy Officer within 24 hours of being alerted under 3.1.

3.3 Privacy Officer to issue pre-emptive instructions

On receipt of the communication by the relevant member of the Province Administration under 3.2, 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 Data Breach Response Team (Response Team). This will depend on the nature and severity of the breach.

3.3.1 Data breach managed at the Order Level

Where the Privacy Officer instructs that the data breach is to be managed at the local level, the relevant Member of the Province Administration 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); and
- submit a report via the Privacy Coordinator within 48 hours of receiving instructions under 3.3. 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 will be logged in Alfresco (OSA's Document Management System) by the Privacy Officer.

3.3.2 Data breach managed by the Response Team

Where the Privacy Officer instructs that the data breach must be escalated to the Response team, the Privacy Officer will convene the Response Team and notify the Prior Provincial.

The Response team will consist of:

- Privacy Officer
- Province Administrator (or nominee)
- Prior Provincial (or nominee)
- IT Support Contractor (or nominee)

3.4 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 3.2.1 and 3.2.2 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 (with reference to section 3.2.2 above and section 26WG of the NDB Act).
- 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 members of the province, staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.

The Privacy Officer will provide periodic updates to the Prior Provincial, or as deemed appropriate.

3.5 Notification

Having regard to the Response team's recommendation in 3.4 above, 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).

If practicable, OSA must also notify each individual to whom the relevant personal information relates. Where impracticable, OSA must take reasonable steps to publicise the statement (including publishing on the OSA.org.au website if required).

The prescribed statement will be logged by the Privacy Co-ordinator.

3.6 Secondary Role of the Response Team

Once the matters referred to in 3.4 and 3.5 have been dealt with, the Response team should turn attention to the following:

- Identify 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.
- Prepare a report for submission to the Prior Provincial and/or The Provincial Council
- Consider the option of an audit to ensure necessary outcomes are affected and effective.

4. Updates to this Procedure

In line with OSA's Policy Development, this procedure is scheduled for review every five years or more frequently if appropriate.

5. Revisions made to this document


<u>Date</u>	<u>Major / Minor Revision</u>	<u>Description of Revision(s)</u>
November 2018	Major	Policy Submission and approval request to the Provincial Council

6. Contact details

Contact for all matters related to privacy, including complaints about breaches of privacy, should be directed as follows:

Professional Standards Officer/Privacy Officer: Fr. David Austin OSA

Email: dave.austin@osa.org.au

: 02 9938 0200

P: PO Box 7278 Warringah Mall, Brookvale 2100