Data Breach Notification Policy

1. Purpose

The Privacy Act imposes ongoing obligations to take reasonable steps to handle personal information in accordance with the Australian Privacy Principles. This includes protecting personal information from misuse and interference and loss, and from unauthorised access, modification or disclosure.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Commonwealth) incorporates mandatory data breach notification requirements into the *Privacy Act 1988* (Commonwealth).

To ensure ANC is compliant with our obligations under these requirements, this Policy sets out ANC's requirements for managing data breaches that impact Personal Information collected. The five key steps are outlined below.

Most importantly, the aim of this Policy is to enable our employees and contractors to:

- have open and prompt dialogue when suspecting, assessing and managing data breaches;
- work together to remediate and minimise the risk of harm to individuals whose personal information is impacted by data breaches;
- comply with our notification responsibilities to the OAIC and affected individuals; and
- implement prevention plans to prevent data breaches from reoccurring.

2. Scope

This policy applies to all employees, consultants and sub-contractors (contractors) of ANC.

3. Definitions

Personal Information	Includes any information provided to ANC about an identified individual or an individual who can be reasonably identified from the information (personal information can be in any format e.g. images of individuals in photographs or video will be personal information where the person's identity is clear or can be reasonably worked out from the image)
Data breach	Occurs when there is unauthorised access to, or unauthorised disclosure or loss of personal information
Notifiable Incident	Any incident where an employee or contractor becomes aware of any grounds to believe or suspect that there has been unauthorised access to, or disclosure or loss of, Personal Information
OAIC	Office of the Australian Information Commissioner
Privacy Act	the Privacy Act 1998 (Cth)

4. Action to Take in the Case of a Notifiable Incident

In most cases of a data breach, ANC's technical support provider (MOSAIC) will be the first to identify a breach. MOSAIC will follow agreed actions to assist ANC to undertake the required notification, management and remediation steps, in line with this policy and current privacy legislation.

Where an employee or contractor identifies or suspects a data breach has occurred, there are five key steps to follow:

- Notification
- Remediation
- Investigation and Reporting
- Assisting ANC
- Prevention

5. Notification

Employees and contractors will immediately notify ANC through their State Manager as soon as they become aware of any grounds to believe or suspect that a Notifiable Incident has occurred.

If in any doubt as to whether to notify ANC of an incident, the employee/contractor must contact their State Manager or National Manager Operations as soon as practicable in order to have an open and prompt dialogue and if necessary, obtain further guidance. Current State and National Manager contact details are provided at the end of this document.

When notifying ANC of any Notifiable Incident, employees/contractors need to provide as much of the following information as is known, including:

- the nature and details of the notifiable Incident
- possible impact of the notifiable Incident
- preliminary actions and recommendations

A Data Breach Notification template is available to support this action (Appendix A and SharePoint).

6. Remediation

Immediately after becoming aware of the data breach or suspected data breach, the State or National Manager will take all necessary and appropriate action to:

- contain the data breach e.g. stop the unauthorised practice or recover the records;
- mitigate potential loss or interference with Personal Information;
- prevent harm to individuals as a result of the breach; and
- protect the information from any further misuse, loss, access or disclosure.

7. Investigation & Reporting

Immediately following notification to ANC, the State or National Manager will:

- appoint an incident manager to lead the initial assessment;
- investigate and complete an assessment of the Notifiable Incident (to the extent then known), within three (3) calendar days;
- identify and agree the steps available to contain the breach and action any agreed steps as soon as practicable; and
- provide ongoing updates on results of the investigation, assessment and recommendations.

8. Assisting ANC

Immediately following notification to ANC, employees, contractors and State Managers will:

- provide all reasonable assistance requested by the incident manager in conducting the investigation and management of the Notifiable Incident; and
- comply with ANC's reasonable directions in connection with management of the Notifiable Incident, including in relation to the prevention of future incidents.

Additionally, the State or National Manager will:

- work with ANC Executive to determine whether the Notifiable Incident is likely to result in serious harm to affected individuals and therefore requires notification to the OAIC and affected individuals;
- allow ANC Executive to control the process of assessing and notifying affected individuals, clients and the OAIC.

9. Prevention

Once:

- a Notifiable Incident is contained;
- risk of immediate harm is mitigated; and
- any required notifications to the OAIC and affected individuals and clients are issued,

the Incident Manager, State or National Manager will prepare a final report which specifies:

- the root cause of the Notifiable Incident; and
- the corrective actions to be undertaken to prevent a repeat occurrence of the Notifiable Incident.

The State or National Manager will ensure implementation of the prevention plan.

10. Examples of Data Breach and Remediation Activities

Example 1:

A data file, which includes the personal information of numerous individuals, is sent to an incorrect known recipient outside ANC. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed. The sender then advises the recipient that the file is not intended for them and confirms that the recipient has not copied, and has permanently deleted the data file (including, if necessary, by obtaining a Statutory Declaration from the recipient).

Example 2:

A contractor leaves their manifest (run sheet) in a public space while going about their delivery work. A short while later, the contractor realises that the manifest has been lost. While backtracking to the most recent delivery site to search for the manifest, the contractor calls ANC to alert their Allocation/Despatch team member who escalates to the ANC State or National Manager. The manifest is located at the delivery site. Because of the quick action of the contractor, they can continue on their way and the ANC State or National Manager is confident that the manifest's information could not have been accessed in the short period between when it was lost and when it was found.

11. Corrective Action

Deliberate neglect to comply with this policy is an act of serious and wilful misconduct and may result in the immediate termination of the employee's employment contract and may also result in prosecution. Failure to comply with this policy may result in an investigation and application of corrective actions including possible termination of employment, legal action, and criminal liability.

12. Current State Manager Contact Details

A current list of State Managers for notification of possible data breach (as at December 2018):

LOCATION	ROLE	NAME	PHONE
ACT	State Manager	Andy Queck	0432 547 053
NSW	State Manager	Sheryl Christensen	0409 830 270
QLD	State Manager	Kristian Houe	0431 793 484
SA	State Manager	Sam Rhodes	0438 897 489
VIC	State Manager	Brooke Cracknell	0459 856 907
WA	State Manager	Sam Rhodes	0438 897 489
NATIONAL	National Manager Operations	Kylee Bidwell	0477 711 732

13. References

Related internal and external guidance includes:

- *ANC Privacy Policy Statement*

For further guidance on mandatory data breach notification under the Privacy Act, please refer to the Office of the Australian Information Commissioner's (OAIC) website: www.oaic.gov.au

Appendix: Data Breach Notification Template

Incident Name	
Incident Description e.g. details of what type of personal information is affected (or suspected to be affected) and the number of individuals who could be impacted	
Any security measures on Personal Information e.g. encrypted, anonymized, not easily accessible	
Date Incident Occurred	
Date Incident Detected	
Incident Identified by	
Contact Details	
Root Cause e.g. malicious or criminal attack, system fault, human error	
Preliminary Actions e.g. any action taken to contain a data breach and/or remedial action that prevents the likelihood of serious harm occurring for any individuals whose personal information is involved in the data breach	
Recommendations e.g. recommendations for any actions that may be taken by ANC, MOSAIC or others in order to mitigate the impact of the breach	