DATA BREACH RESPONSE PLAN

Created: October 2024 | Last Amended: October 2024 | Next Review: October 2027

Maintain information governance and security - APP 1 and 11

NNSW Conference 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 NNSW Conference holds.

Contain

NNSW Conference'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

NNSW Conference 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 NNSW Conference 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, NNSW Conference should consider whether **remedial action** is possible.

NNSW Conference should consider adopting OAIC's suggested three-stage process:

- **Initiate:** plan the assessment and assign a team or person (General Secretary)
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. (document this).

NNSW Conference 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, NNSW Conference 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 accounts before unauthorised transactions can occur. If remedial action is successful in making serious harm no longer likely, then notification is not required and NNSW Conference can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, NNSW Conference must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the NNSW Conference's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals.

NNSW Conference 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 NSW Conference's website and publicise it

NNSW Conference 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

NNSW Conference 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
- Their financial services provider

NNSW Conference that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.