TEMPLATE DATA BREACH RESPONSE PLAN

Adopted: June 2023 Last Amended: Next Review: June 2025

Maintain information governance and security – APP 1 and 11

Schools 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

Contain

Contain a suspected or known Data Breach where possible.

Assess

Schools 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 School has reasonable grounds to believe this is the case, then this is an **EDB** and it must notify individuals affected and the Information Commissioner. If it only has grounds to suspect that this is the case, then it must conduct an **assessment**. As part of the assessment, Schools should consider whether remedial action is possible.

Schools should consider adopting the OAIC's suggested a three-stage process:

Initiate: plan the assessment and assign a response 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 (and document this).

Schools should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30days, document why this was the case.

Take remedial action

Where possible, a School should take steps to reduce any potential harm to individuals. For example, this might involve taking action to recover lost information before it is accessed or changing access controls on accounts before unauthorised transactions can occur. If remedial action is successful in making serious harm no longer likely, then notification is not required and Schools can progress to the review stage.

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

Notify

Where serious harm is likely, a School must prepare a statement for the Commissioner (a form available on OAIC website) that contains:

- the School's identify and contact details
- a description of the Data Breach the kind/s of information concerned
- recommended steps for individuals affected

Schools 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 School's website and publicise it

Schools can provide further information in their notification, such as an apology and an explanation of what they are doing about the Data Breach. **In some limited circumstances, an exception to the obligation to notify the individuals or the Commissioner may apply.**

Review

Review the incident and take action to prevent future Data Breaches. This may include:

- Fully investigating the cause of the Data Breach
- Developing a prevention plan
- Conducting audits
- Updating security/response plan
- Considering changes to policies and Procedures
- Revisiting staff training practices

Schools should also consider reporting the incident to other relevant bodies, such as:

- Police or law enforcement
- Other external or third parties (eg the ATO)
- The Australian Cyber Security Centre and related agencies
- Professional bodies
- Credit card companies or financial services providers

Schools that operate outside Australia may have notification obligations under other breach notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.