The Uniting Church in Australia
QUEENSLAND SYNOD

Tool

Data Breach Incident Notification Form

B/1.1.2.1

Purpose

A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information. This Data Breach Incident Notification Form sets out contact details for the appropriate staff in the event of the data breach, clarifies the roles and responsibilities of staff and documents processes to assist The Uniting Church in Australia, Queensland Synod to respond to a data breach.

Scope

This form will assist The Uniting Church in Australia, Queensland Synod staff in documenting the process where data breach occurs, or is suspected, as outlined in the Data Breach Response Plan Procedure (the Procedure). If assistance is required in completing this form, please contact the Synod Privacy Officer (Privacy@ucaqld.com.au) immediately.

Alert

Upon becoming aware of an actual or potential data breach, the relevant staff member is required to alert his/her Person Responsible within the relevant timeframe1 of a data breach, or a suspected breach, in accordance with Section 4 of the Procedure. [If in doubt, better to err on side of caution and notify the Person Responsible].

Date of Breach:	DD.MM.YYYY
Time when Breach was first noticed:	00:00 am/pm
Description of Breach:	*[describe the type of personal information involved eg contact details, date of birth]*
Cause of Breach:	*[if unknown, explain how the data breach was discovered]*
Which system(s), if any, are affected?	
Which Synod entity is involved?	
Has corrective action occurred to remedy or ameliorate the breach or suspected breach? If so, what?	
Alert made by:	*[Name of staff member]*
Date:	DD.MM.YYYY

Once completed, send to Person Responsible

[1] A list of Persons Responsible and relevant timeframes are set out in Table A under Section 4 of the Data Breach Response Plan Procedure

Assessment and Determination of Potential Impact

The Person Responsible must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The Synod Privacy Officer may be contacted for advice.

If the data breach or suspected data breach is considered minor (ie not a likely risk of serious harm), then the Person Responsible is to ensure the Data Breach Incident Form is completed with their Assessment and Determination and sent to the Synod Privacy Officer within the relevant timeframe of receipt of the Alert, in accordance with Section 4 of the Procedure.

Alert received by:	
Name:	[Name of Person Responsible]
Date:	DD.MM.YYYY
Criteria for determining whether a privacy data breach has occurred	
Is personal information involved?	Yes ☐ No ☐
Is the personal information of a sensitive nature?	Yes ☐ No ☐
Has there been unauthorised access to personal information, or disclosure or personal information, or loss of personal information in circumstances where access to the information is likely to occur?	Yes ☐ No ☐
Criteria for determining severity	
Describe the type and extent of personal information involved:	Provide further details:
Have multiple individuals been affected?	Yes ☐ No ☐ If yes, provide further details:
Confirm whether the information is protected by any security measures and, if so, describe those security measures:	
Provide details of the person or kinds of people who now have access:	
Determine whether there is (or could be) a real risk of serious harm to the affected individuals. Set out your determination and reasoning:	
Determine whether there could be media or stakeholder attention as a result of the breach or suspected breach:	

Determination: Likely risk of Serious Harm / Minor

If Minor: Send to Synod Privacy Officer

If Not Minor: Send to Synod Office Duty Officer (synodoffice.dutyofficer@ucaqld.com.au) with a copy to Synod Office Privacy Officer (Privacy@ucaqld.com.au).

Pre-emptive instruction by Synod Privacy officer

If the data breach is deemed serious enough, the Synod 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 Incident Response Team, depending on the nature and severity of the breach.

Notification received by:	
Name:	[Name of Synod Privacy officer]
Date:	DD.MM.YYYY
Determination:	
How the data breach is to be managed:	Person Responsible OR Data Incident Response Team
Any further instructions issued by the Synod Privacy Officer:	
Date of instruction:	DD.MM.YYYY

If data breach managed at the Person Responsible level

Description of breach:	
Action taken:	
Outcome of Action	
Processes implemented to prevent a repeat of the situation	
Any other information of relevance	
Recommendation to the Synod Privacy officer	Example: No further action is necessary
Report submitted by:	
Date:	[Name of Synod Person Responsible]
Synod Privacy Officer's determination that no further action is necessary	Yes ☐ No ☐
Signed:	[signature of Synod Privacy officer]
Date:	

Related documents

Data Breach Response Plan Procedure

Revisions

Document number		B/1.1.2.1			
Version	Approval date	Approved by	Effective date	Policy owner	Policy contact
1.0	08.06.2018	New Process Form	11.06.2018	Executive Director Risk	Privacy Officer
1.1	24.01.2023	Policy owner change	25.01.2023	General Secretary	Privacy Officer
Next scheduled review		24.01.2025			