The Uniting Church in Australia
QUEENSLAND SYNOD

Procedure

Data Breach Response Plan Procedure

B/1.1.2

1. Introduction

The cost to the Uniting Church in Australia, Queensland Synod and the Uniting Church in Australia Property Trust (Q.) (collectively hereinafter referred to as the UCAPT(Q)) for a data breach can be significant and could include damage to reputation and significant costs and statutory penalties.

2. Scope

This procedure applies to all entities and institutions of UCAPT(Q) and any other entity engaged in an activity of the Queensland Synod.

This procedure:

a. Provides the systematic processes that should be undertaken by any entity of the UCAPT(Q) in the event that a data breach is suspected, discovered or reported.

b. Is intended to enable UCAPT(Q) to contain, assess and respond to data breaches in a timely fashion, and to help mitigate potential harm to affected individuals.

c. Will assist UCAPT(Q) to comply with relevant obligations under the *Privacy Act 1988* (Cth) and particularly Part IIIC, Division 3, *Notification of eligible data breaches*, pertaining to notifying the Privacy Commissioner and the individuals to whom the relevant information relates of the data breach.

d. Aims to better protect important business assets and enable us to deal with adverse media or stakeholder attention from a breach or suspected breach; and instil confidence of UCAPT(Q)'s capacity to respond appropriately.

3. Principles

a. It is essential that all parties involved in breach reporting, investigation and rectification act in good faith to obtain a satisfactory outcome.

b. No blame should be attached to the person reporting accidental breaches or those identifying process errors.

c. Individuals committing deliberate or negligent breaches maybe subject to disciplinary processes within UCAPT(Q) or regulatory/criminal actions (where applicable and/or appropriate).

d. Breaches or potential breaches can be reported anonymously. If information is received in this manner, the response should be in accordance with this procedure.

e. Data breaches need to be considered on a case-by-case basis. The five key steps involved in responding to a breach or suspected breach:
Step 1: Contain the breach and do a preliminary assessment
Step 2: Eliminate the circumstances enabling the breach
Step 3: Evaluate the risks associated with the breach
Step 4: Notification
Step 5: Prevent future breaches

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

4. Initial Identification and Notification

1. Ministry agents, lay staff and volunteers will notify the relevant Person Responsible (See Table A) immediately of the breach or potential breach.

Table A

Area of UCAPT(Q)	Recipient of notification/Person Responsible	Timeframe to be notified
Schools	Head of School Head of School to notify Executive Officer for Schools and Residential Colleges	For serious suspected breach: Immediately Other suspected breach: as soon as is practicable
UCQ and WMQ	Person in control of a workplace (e.g. line manager) to notify CEO	For serious suspected breach: Immediately Other suspected breach: as soon as is practicable
Business Groups of the Synod Office	Executive Director	For serious suspected breach: Immediately Other suspected breach: as soon as is practicable
Congregations (incl Ministry Agent)	Presbytery Minister	For serious suspected breach: Immediately Other suspected breach: as soon as is practicable
Any other Entity of the Synod	Head of Entity	For serious suspected breach: Immediately Other suspected breach: as soon as is practicable

5. What constitutes an 'eligible data breach'

1. There has been unauthorised access to, or unauthorised disclosure of, Personal Information and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates;
2. Personal Information is lost and unauthorised access to, or unauthorised disclosure of, the information is likely to occur and if this were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

6. Assessment of 'suspected' data breach

If reasonable grounds to suspect a data breach arise but not reasonable grounds to believe a data breach has occurred, then an expeditious and thorough assessment is to be undertaken to determine whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. All reasonable steps will be taken to ensure the assessment is completed within 30 days after becoming aware of the suspicion.

7. Breach Containment

Person responsible: As defined in Table A. Timeframe: Immediately or as soon as is practicable after notification.

The breach containment should include:

a. Common sense steps to limit or contain the breach.
b. Do not compromise the ability of any resulting investigation
c. Do not destroy evidence that may be valuable in determining the cause or allow corrective action to be taken.

8. Breach Assessment and Escalation

Person Responsible: As defined in Table A will:

1. Evaluate if the breach is potentially a 'likely risk of serious harm' or 'Minor' in the context of the following questions:
   a. The kind or kinds of information.
   b. The sensitivity of the information.
   c. Whether the information was protected by one or more security measures.
   d. If the information was protected by one or more security measures – the likelihood that any of those security measures could be overcome.
   e. The persons, or the kinds of persons, who have obtained, or who could obtain, the information.
   f. If a security technology or methodology:
      - was used in relation to the information; and
      - was designed to make the information unintelligible or meaningless to person who are not authorised to obtain the information,

      the likelihood that the person, or 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.
   g. The nature of the harm.
   h. Could multiple individuals be affected?
   i. Could there be potential for a likely risk of serious harm to affected individuals?
   j. Is there a systematic deficiency in the organisation's Privacy processes or procedures?
   k. Is potential Media or stakeholder attention anticipated?
   l. Could intellectual property be jeopardised?
   m. Could the impact on UCAPT(Q) include investigation by a regulator or statutory body and/or potential for a sanction, enforceable undertaking, fine, penalty, compensation payment?
   n. Any other relevant matters.

2. Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.

3. All confirmed or suspected data breaches must be recorded.

   a. Any breach that presents a 'likely risk of serious harm' must be escalated. The Person Responsible in Table A is responsible to escalate 'likely Risk' matters relevant to their area. If the answer to any of aforementioned questions is 'yes', then this would constitute a 'likely risk of serious harm' breach, and it is appropriate for the Person Responsible in Table A to immediately notify the Office of the General Secretary.

4. If the Person Responsible in Table A decides that a data breach or suspected data breach is minor (i.e. not likely risk of serious harm), then the Person Responsible in Table A is to ensure the Form: Data Breach Incident is completed and sent to the Synod Privacy Officer (Synod General Counsel).

5. If the data breach or suspected data breach is not minor, then an appropriate investigation should be undertaken to inform the outcome.

6. The General Secretary/Person Responsible will determine whether any data breach is deemed serious enough to constitute invoking the Data Incident Response Team to manage the situation and/ or the appropriate avenue for investigation.

7. If the privacy breach is deemed serious enough to constitute the Data Incident Response Team, then the constituents of the Data Incident Response Team will be called upon to respond depending on the nature of the breach and context of the breach. In more serious cases, external experts may be required to be engaged. Potential membership of the Data Incident Response Team is listed in Table B.

Data Incident Response Team Membership (Table B)

Indicative title	Responsibility
Team Leader – Either the head of Risk, or the UCAPT(Q) Privacy Officer	Oversee Data Incident Response Team External contact point for the Office of the Information Commission for reporting requirements
Legal Advisor	To assist to identify legal obligations and provide advice
Risk and Compliance Manager	To support in the assessment of the risks from the breach and investigation
Manager People & Culture	Provision of support in the event the action was due to a staff member
Manager – Communications & Marketing	Expertise to assist in communicating with affected individuals and dealing with the media and external stakeholders
IT Manager – acting in the capacity of Synod Information Security Officer	Assist in review of security and monitoring controls related to the breach (for example, access; authentication; encryption; audit logs) and support involving investigation of IT systems
Manager – Group Insurance	Provide liaison with Brokers and Insurers

Where there is a significant event within Wesley Mission Queensland (WMQ) or UnitingCare Queensland (UCQ) to invoke their respective Data Incident Response Team, the Manager – Group Insurance is to be a team member, and the Executive Director Risk or UCAPT(Q) Privacy Officer to be a team member to provide liaison between WMQ and UCQ and the UCAPT(Q).

9. Investigation

The investigation should commence immediately after the breach has been assessed and contained and be carried out thoroughly and as expeditiously as is reasonable.

The level of investigative effort should reflect the seriousness of the breach. Investigations should determine the root causes; identify whether it was a systemic breach, an isolated incident or a deliberate act; identify and gain agreement on the appropriate actions to prevent the breach recurring or escalating to a more serious level; apply the principles of natural justice and be completed in a timely manner.

The investigation outcome should be reported to the appropriate manager and details included in the Data Breach Incident Notification Form. Where breaches involve criminal activity, this should be referred to appropriate law enforcement agencies or authorities for investigation.

10. Implementation of Actions

Actions from the investigation should be implemented and include target completion timelines.

Monitoring by the appropriate manager should be undertaken to ensure people identified as responsible for implementation of actions are completing actions on or before the required timeline.

11. Breach Recording/ Register

A central register of data breaches or potential data breaches will be maintained by the Office of the General Secretary through the Synod Privacy Officer. The register will include a record of all reported breaches/ potential breaches and investigation outcomes.

12. Breach Notification

If at any time after being notified of a Breach or Suspected Breach, the General Secretary forms the opinion that serious harm to affected individuals is likely, a notification is to be made to the affected individuals and the Office of the Australian Information Commissioner in conformity with the notification obligations set out in the *Privacy Act 1988* (Cth).

In considering notification the General Secretary will have regard to whether or not serious harm is likely, that is, more probable than not. In deciding whether this is the case, regard will be given to the list of 'relevant matters' set out in section 26WG of the PrivacyAct.

13. Post-review

Following a 'likely risk of serious harm' breach, a post-breach review will be conducted by the Data Incident Response Team to assess the response to the data breach and the effectiveness of the data response plan.

14. Testing the Response

The Data Breach Response Procedure should be tested on a regular basis.

15. Records Management

All Data Breach Notification forms and documents created by the Data Incident Response Team should be saved in the electronic document repository used by the Office of the General Secretary.

16. Definitions

TERM	MEANING
Queensland Synod	Means the work and activities of the Uniting Church in Australia performed within the bounds of the Queensland Synod.
Person Responsible	Means the Head of an Entity engaged in an activity of the Queensland Synod.
Data Breach	Personal information held by an entity (in any form including both hard media and electronic) is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. A 'data breach' may also constitute a breach of the *Privacy Act 1988* (Cth).

Likely Risk of Serious Harm	A breach or suspected breach to which any of the following could apply: • Multiple individuals could be affected • There could be potential for a real risk of serious harm to affected individuals • A systematic problem in the organisations Privacy processes or procedures is revealed or suspected • Media or stakeholder attention might be anticipated • Intellectual property may be jeopardised • the impact on UCAQ may include investigation by a regulator or statutory body and/or potential for a sanction, enforceable undertaking, fine, penalty, compensation payment • Other relevant factors: - 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: (i) was used in relation to the information; and (ii) 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: (iii) have obtained, or who could obtain, the information; and (iv) 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; (i) the nature of the harm; (j) any other relevant matters.

17. Related Documents

Relevant Legislation / By-Laws / Standards:
Privacy Act 1988 (Cth)

Related documents:

The Privacy Policy – Policy Statement B1.1

The following advisory chart from the Office of the Information Commissioner (OIC) provides further context to this Data Breach Process.

Maintain information governance and security — APP 1 and 11

Entities 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 an entity holds.

Contain

An entity'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

Entities 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 entity 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, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a 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. OAIC recommends that this be documented.

Entities 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, an entity 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 customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

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

Notify

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

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

Entities 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 entity's website and publicise it

Entities 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

Entities 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
- your financial services provider

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

18. Revisions

Document number		B/1.1.2			
Version	Approval date	Approved by	Effective date	Policy owner	Policy contact
1.0	02.03.2018	General Secretary	03.03.2018	Executive Director Risk	Synod Privacy Officer
1.1	24.01.2023	Policy owner change	25.01.2023	General Secretary	Synod Privacy Officer
Next scheduled review		24.01.2025			