QUEENSLAND PERFORMING ARTS CENTRE

DATA BREACH POLICY

DOCUMENT CONTROL

Document Name:	Data Breach Policy		
Document ID:	GOV-POL-202509-0137-1.0		
Version:	1.0		
Approved by:	Chief Executive	**Date approved:**	5 September 2025
Maintained by:	General Counsel	**Date of next review:**	5 September 2028

CONTENTS

CONTEXT

1. QPAC is an Agency for the purposes of the *Information Privacy Act 2009* (Qld) (IP Act) and is required to ensure that all Personal Information under QPAC's control is protected against loss, unauthorised access, modification, disclosure or any other misuse.

2. The IP Act establishes a mandatory notification of data breach (MNDB) scheme which imposes the following key obligations on agencies with respect to Eligible Data Breaches and Suspected Eligible Data Breaches:

   (a) contain the Data Breach;

   (b) mitigate the harm caused by the Data Breach;

   (c) notify the Information Commissioner and particular individuals where an Agency believes the data breach is an Eligible Data Breach;

   (d) prepare and publish a Data Breach Policy; and

   (e) keep a register of Eligible Data Breaches.

PURPOSE

3. The purpose of this Policy is to:

   (a) outline QPAC's approach to preparing for, responding to and recovering from a Data Breach, in particular an Eligible Data Breach or a Suspected Eligible Data Breach; and

   (b) ensure that QPAC complies with its obligations under the IP Act with respect to the MNDB scheme.

APPLICATION

4. This Policy applies to all Employees.

5. Neither this Policy nor any part of its contents forms part of any person's contract of employment or engagement or creates, or forms part of, any contract between any other party to whom this Policy applies and QPAC.

6. QPAC may, in its absolute discretion, amend this Policy at any time.

SCOPE

7. The scope of this Policy is limited to Data Breaches involving Personal Information held by QPAC, which is information that is contained in a document in QPAC's possession or under the control of QPAC. This includes Personal Information held by QPAC's ticketing service, QTIX.

8. Data Breaches that do not involve Personal Information will be handled in accordance with QPAC's other policies and procedures, such as the Cyber Security Incident Response Plan or Emergency Management Plan.

POLICY

Preparation

9. QPAC maintains the following policies and plans to inform its approach to cultivating a robust information security environment and ensuring QPAC is well-positioned to respond to information security incidents:

   (a) Cyber Security Incident Response Plan;

   (b) Emergency Management Plan;

   (c) ICT Acceptable Use Policy;

   (d) Information Security and Data Management Policy; and

   (e) Records Management Policy.

10. The abovementioned policies and plans may also be consulted in the event Data Breach, where relevant.

11. Employees will be required to undertake training on information security, including how to identify and report a Data Breach. Annual refresher training will be mandatory for all Employees who access Personal Information as part of their usual role requirements.

Roles and Responsibilities

12. QPAC has assigned the following roles and responsibilities to effectively manage a Data Breach:

Role	Responsibility
Employee	Read the Data Breach Policy and understand what is required of them. Complete training on information privacy, specifically QPAC's obligations under the IP Act and the MDBN scheme. Comply with the IP Act, including protecting Personal Information held by QPAC from unauthorised access, disclosure or loss. Where required in accordance with this Data Breach Policy, immediately report a Data Breach to their Manager. Comply with record keeping obligations.
Manager	Champion strong information security practices in their respective teams. Escalate Data Breaches reported by an Employee to the Chief Information Officer and Privacy Officer as required.
Privacy Officer (QPAC General Counsel)	Assess the severity of a Data Breach involving Personal Information to determine whether the Data Breach is a Suspected Eligible Data Breach or Eligible Data Breach. Notify the Information Commissioner and ensure QPAC's other notification obligations under the MNDB scheme are

Role	Responsibility
	satisfied in the event of an Eligible Data Breach. This includes publishing, monitoring and reviewing the currency of public notifications of a Data Breach published to the Agency website under section 53(1)(c). Maintain the Register of Eligible Data Breaches.
Chief Information Officer (QPAC Chief Financial Officer)	Responsible for overall management of QPAC's information security systems. Convene the Data Breach Response Team, when appropriate. Immediately report a cyber security incident that is also a Data Breach to the Privacy Officer, if not already reported. Oversee and coordinate QPAC's response to a Data Breach, including identified containment and mitigation measures
Manager ICT	Monitor QPAC's ICT systems to ensure the swift detection of Data Breaches. Implement containment and mitigation measures for Data Breaches involving QPAC's electronic systems.
Data Breach Response Team: • Privacy Officer • Chief Information Officer • Manager – ICT • Executive Director – People and Culture • Communications Manager • Network and Systems Support Manager • Systems Administrators (as required for cyber Data Breaches) • Other management personnel responsible for the business unit in which the Data Breach occurred	Convene, as required, to discuss actions required to manage a Suspected Eligible Data Breach or Eligible Data Breach. Support the identification, containment, assessment, notification and post Data Breach review process in accordance with this Policy. Ensure appropriate records of actions and decisions are taken.
External Service Providers	Specialist technical advice and remediation for the detection and management of Data Breaches, as required.
Communications Manager	Draft and coordinate the delivery of the following communications in relation to Data Breaches: • Internal communications to Employees; and • External communications to Affected Individuals, relevant stakeholders and the general public.

13. A list of contract details of the Data Breach response Team and relevant external service providers, and a copy of this Policy will be accessible online and in secure physical locations.

Identification

14. The following processes will guide QPAC's approach to detecting, identifying and escalating a Data Breach.

Key Terms

15. A Data Breach means either of the following in relation to information held by QPAC:

    (a) unauthorised access to, or disclosure of, the information; or

    (b) loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

16. Examples of a Data Breach may include the following:

    (a) a cyberattack, phishing, malware or hacking incident into a QPAC system, allowing access by external parties;

    (b) inappropriate access by an Employee to a restricted internal file containing Personal Information;

    (c) QPAC disclosing an individual's Personal Information to a third party who is not the intended recipient. or

    (d) an Employee accidentally losing a laptop or physical documents containing Personal Information.

17. For a Data Breach to be an Eligible Data Breach, the two following criteria must be met:

    (a) there is unauthorised access to, or unauthorised disclosure of, Personal Information held by QPAC, or there is a loss of Personal Information held by QPAC in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and

    (b) the unauthorised access to, or disclosure of the information is likely to result in Serious Harm to an individual to whom the Personal Information relates.

18. A Suspected Eligible Data Breach is a Data Breach that QPAC knows or reasonably suspects to be an Eligible Data Breach.

Detection

19. All Employees must understand what constitutes a Data Breach and an Eligible Data Breach.

20. If an Employee becomes aware of a Data Breach, they must immediately notify their Manager.

21. If a Manager is notified or becomes aware of a Data Breach that involves, or they suspect may involve, Personal Information, they must immediately notify the Chief Information Officer and the Privacy Officer.

22. Data Breaches may also be detected by third-party security providers engaged to monitor and detect threats to QPAC's online information environment.

23. QPAC ensures that that any third parties with access to Personal Information held on QPAC's behalf are contractually obliged to notify QPAC in the case of a Data Breach involving such Personal Information.

Initial Assessment

24. The Chief Information Officer and Privacy Officer will notify each other respectively of any Data Breach that involve Personal Information as soon as practicable after being made aware of the Data breach.

25. The Privacy Officer will determine whether the Data Breach involves Personal Information. If the Data Breach does not involve Personal Information, the remaining provisions of this Policy do not apply.

26. The Privacy Officer will make an initial determination on whether the known circumstances of the Data Breach support a reasonable suspicion that the Data Breach is a Suspected Eligible Data Breach or Eligible Data Breach.

27. If the Privacy Officer determines that a Suspected Eligible Data Breach or Eligible Data Breach has occurred, the Data Breach Response Team will be stood up and steps 3 – 6 of this Policy will be actioned.

28. If the Privacy Officer determines that the Data Breach is not an Eligible Data Breach or Suspected Eligible Data Breach, the Data Breach will be managed in accordance with QPAC's other relevant policies and procedures.

29. If at any time QPAC becomes aware that the Data Breach affects another Agency that is subject to the IP Act, QPAC will provide that Agency with written notice of the breach, including the following:

    (a) a description of the Data Breach; and

    (b) a description of the kind of Personal Information that may be the subject of the Data Breach, without including any of the Personal Information itself.

Containment/Mitigation

30. In the event of a Suspected Eligible Data Breach or Eligible Data Breach, the Data Breach Response Team will convene as soon as practicable to determine the reasonable steps QPAC will take to contain and mitigate the effects of the Data Breach.

31. A data breach response run sheet will be opened and updated for the duration of the handling of the Data Breach. The Privacy Officer will delegate a member of the Data Breach Response Team to act as scribe to maintain the data breach response run sheet and record key actions and decisions.

32. Containment and Mitigation measures will seek to minimise harm to the individuals whose Personal Information the Data Breach relates to and protect any QPAC systems that have been compromised by the Data Breach.

33. The Data Breach Response Team may consider implementing the following steps to contain and mitigate the Data Breach:

    (a) implementing internal controls;

    (b) suspending the activity that led to the Data Breach;

    (c) making immediate efforts to recover the Personal Information;

(d) securing, restricting access to or shutting down breached systems;

(e) working with External Service Providers to investigate and resolve the incident

(f) determining the cause the incident; or

(g) revoking or changing passwords.

34. The Chief Information Officer will coordinate with the relevant Manager and System Administrators to implement the appropriate containment and mitigation measures agreed by the Data Breach Response Team.

35. The Chief Information Officer will provide continuous updates to the Data Breach Response Team and update containment and mitigation measures through consultation with the Data Breach Response Team where necessary.

4. Assessment

36. As soon as sufficient information of the impacts of the Data Breach are known, the Privacy Officer will coordinate an assessment of the Data Breach in accordance with this section of the Policy to determine whether the Breach is an Eligible Data Breach.

37. The assessment will be completed within 30 days of the date when QPAC first had reasonable suspicion of a Data Breach.

38. The Privacy Officer will liaise with the Chief Information Officer, the Data Breach Response Team, the Executive Director of the Business Unit where the Data Breach occurred, and any other relevant stakeholders to gather information relevant to the circumstances of the breach, including the type of Personal Information involved and the individual/s the Data Breach relates to.

39. The Privacy Officer will determine whether the Data Breach is likely to result in Serious Harm to an individual to whom the Personal Information relates with regard to the following factors:

(a) the kind of Personal Information accessed, disclosed or lost;

(b) the sensitivity of the Personal Information;

(c) whether the Personal Information is protected by one or more security measures

(d) if the Personal Information is 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 Personal Information;

(f) the nature of the harm likely to result from the Data Breach, and

(g) any other relevant matter.

40. Other relevant matters under paragraph 39(g) may include the following questions:

(a) what is the nature of the Data breach;

(b) is it likely that a counterparty or third party caused the Data Breach;

(c) what is the seriousness of the Data Breach;

(d) has the Data breach affected another Agency subject to the IP Act;

(e) are there any vulnerabilities of the Affected Individuals e.g. involving children or a domestic violence victim-survivor;

(f) the effectiveness of the steps taken to control the Data Breach e.g. has containment and mitigation lessened the risk; and

(g) has there been unauthorised access, disclosure or loss of Personal Information that was collected by the Agency, and if so, would a reasonable person conclude the breach is likely to result in Serious Harm to an individual to whom the information relates.

41. Serious Harm is defined in the IP Act as serious physical, psychological, emotional, or financial harm to the Affected Individual because of the access or disclosure, or serious harm to the Affected Individual's reputation because of the access or disclosure.

42. After considering the above factors in relation to the specific circumstances of the Data Breach, the Privacy Officer will determine whether it is more probable than not that Serious Harm will occur to the individuals whose Personal Information the Data Breach relates to.

Notification

43. If QPAC reasonably believes that there has been an Eligible Data Breach, it will:

(a) prepare and provide a statement to the Information Commissioner containing the information outlined in paragraph 44; and

(b) notify any individuals affected by the breach, including notification of the information outlined in paragraph 45.

Notifying the Information Commissioner

44. QPAC will notify the Information Commissioner as soon as practicable after forming the belief that an Eligible Data Breach has occurred through a written statement including the following information:

(a) QPAC's name and, if another Agency has been affected by the Eligible Data Breach, the name of any other Agency;

(b) whether QPAC is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies

(c) The contact details of the QPAC Employee that the Information Commissioner may contact in relation to the Eligible Data Breach (this will likely be the Privacy Officer);

(d) the date the Eligible Data Breach occurred (if known);

(e) a description of the Eligible Data Breach, including the type of Eligible Data Breach under section 47 of the IP Act;

(f) a description of the kind of Personal Information involved in the Eligible Data Breach, without including any Personal Information in the description;

(g) information about how the Eligible Data Breach occurred;

(h) if the Eligible Data Breach involved unauthorised access to or disclosure of Personal Information, the period during which the access or disclosure was available or made;

(i) the steps QPAC has taken or will take to contain the Eligible Data Breach and mitigate the harm caused to individuals by the data breach;

(j) QPAC's recommendations about the steps individuals should take in response to the Eligible Data Breach;

(k) the total number or, if it is not reasonably practicable to work out the total number, an estimate of the total number of individuals whose Personal Information was accessed, disclosed or lost and affected individuals for the Eligible Data Breach;

(l) whether the notified individuals have been advised how to make a privacy complaint to the Agency under section 166A of the IP Act, and

(m) the total number of individuals notified of the Eligible Data Breach or, if it is not reasonably practicable to work out the total number, an estimate of the total number, if relying on section 57 of the IP Act, the total number of individuals who would have been notified or, if it is not reasonably practicable to work out the total number, an estimate of the total number.

Notifying Individuals

45. QPAC will notify individuals through one of the below options, depending on which option is reasonably practicable in the circumstances, which may involve consideration:

(a) The time, cost and effort required to notify individuals; and

(b) The currency and accuracy of the individuals' contact details.

Option 1: Notify Each Individual

46. If it is reasonably practicable to notify each individual whose Personal Information was accessed, disclosed or lost, QPAC will take reasonable steps to notify each individual of the information outlined in paragraph 49.

Option 2: Notify Each Affected Individual

47. If Option 1 does not apply, QPAC will take reasonable steps to notify each Affected Individual of the information outlined in paragraph 49, if doing so is reasonably practicable.

48. An Affected Individual is someone:

(a) who the Personal Information concerns/relates to; and

(b) who is likely to suffer Serious Harm as a result of the Eligible Data Breach.

Option 3: Publish Information

If Options 1 and 2 do not apply, QPAC will publish the information outlined in paragraph 49 on QPAC's website for a period of at least 12 months. QPAC will inform the Information Commissioner of the location where this information is published.

Required Information for Notifying Individuals

49. QPAC will include the following information in its notice to individuals under Options 1, 2 or 3, to the extent it is reasonably practicable:

(a) the name of QPAC and, if more than one Agency was affected by the Eligible Data Breach, the name of any other Agency;

(b) QPAC's contact details, or the contract details of the QPAC Employee nominated for an Affected Individual to contact;

(c) the date the Eligible Data Breach occurred (if known);

(d) a description of the Eligible Data Breach, including the type of Eligible Data Breach under section 47of the IP Act;

(e) information about how the Eligible Data Breach occurred;

(f) QPAC's recommendations about the steps an Affected Individual should take in response to the Eligible Data Breach;

(g) if the Eligible Data Breach involved unauthorised access to or disclosure of Personal Information, the period during which the access or disclosure was available or made;

(h) the steps QPAC has taken or will take to contain the Eligible Data Breach and mitigate the harm caused to Affected Individuals due to the Eligible Data Breach, and

(i) information about how an individual can make a privacy complaint to QPAC under section 166A of the IP Act.

50. A notification under Options 1 or 2 must include a description of the individual's Personal Information. A notification under Option 3 must include a description of the kind of Personal Information involved in the Eligible Data Breach, without publishing any actual Personal Information.

Exemptions to Notification Obligations

51. The Privacy Officer will determine whether an exemption contained in Chapter 3A, Part 3, Division 3 of the IP Act applies which would mean QPAC is not required to comply with its notification obligations.

Process for Notification

52. The Data Breach Response Team will be consulted to determine the information to be included in QPAC's notification to the Information Commissioner, and the appropriate option for notification to individuals.

53. The Privacy Officer will prepare and send QPAC's notification to the Information Commissioner.

54. The Communications Manager will prepare QPAC's notification to individuals and any other notifications required as part of QPAC's broader communications strategy to respond to the Eligible Data Breach.

55. All notifications must be approved by the Chief Executive prior to being made.

Further Notifications

56. QPAC may determine that notifying other entities of the Eligible Data Breach is appropriate in the circumstances, including the following:

(a) The Queensland Government Insurance Fund (QGIF);

(b) The Queensland Police Service;

(c) The Queensland Government Information Security Virtual Response Team; and

(d) The Minister.

57. QPAC may voluntarily report a Data Breach that does not meet the threshold of an Eligible Data Breach to the Information Commissioner or to individuals whose Personal Information the Data Breach relates to. This may be appropriate in circumstances where individuals would reasonably expect QPAC to notify them of a Data Breach.

Data Breach Register

58. The Privacy Officer will be responsible for ensuring that all Eligible Data Breaches are recorded in QPAC's Eligible Data Breach Register.

Post Data Breach Review and Remediation

59. The Privacy Officer and Chief Information Officer will conduct a review of QPAC's handling of all Suspected Eligible Data Breaches and Eligible Data Breaches (**Data Breach Review**), including the following information:

    (a) Identifying the cause(s) of the breach;

    (b) Analysis of the nature and scale of the breach, including affected systems and data types;

    (c) Summary of mitigation/remediation activities undertaken;

    (d) Assessment of the efficiency and timeliness of the mitigation/remediation efforts;

    (e) Identifications of key learnings from QPAC's response to the Data Breach;

    (f) Evaluation of gaps in existing data protection and breach response measures;

    (g) Identification of areas of improvement for handling Personal Information;

    (h) Review of the effectiveness of QPAC's Data Breach Policy;

    (i) Evaluation of the Response Team's performance and coordination;

    (j) Recommendations for updates to systems, processes and procedures.

60. The Data Breach Review will be shared with the Chief Executive and Data Breach Response Team for consideration and adjustment of QPAC's systems, processes and procedures, where appropriate.

61. All Data Breach Reviews of Eligible Data Breaches will be shared with QPAC's Risk Management and Audit Committee.

ENQUIRIES

62. If you have any enquiries regarding this Policy, please contact:

    (a) your manager; or

    (b) General Counsel.

REVIEW

63. This Policy must be reviewed at least every 3 years.

DEFINITIONS

Term	Definition
Affected Individuals	Affected Individual is defined in paragraph 48 of this Policy

Term	Definition
Agency	As defined in section 18 of the IP Act, that being: (a) a Minister; (b) a department; (c) a local government; or (d) a public authority
Chief Executive	QPAC's Chief Executive (The director of Queensland Performing Arts Trust appointed under section 32 of the QPAT Act)
Chief Information Officer	Chief Financial Officer
Data Breach	Data Breach is defined in paragraph 15
Data Breach Response Team	Data Breach Response Team is as defined in paragraph 12
Eligible Data Breach	Eligible Data Breach is defined in paragraph 17
Employees	All QPAC employees, including permanent, fixed term, casual, full-time, part-time, variable part-time and flexible part-time employees, labour hire staff (employed via a third-party labour hire agency), interns, work experience students and volunteers.
Information Commissioner	Queensland Government Office of the Information Commissioner
IP Act	*Information Privacy Act 2009* (Qld)
Manager	An Employee who has line management responsibility for other Employee/s
Personal Information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not
Privacy Officer	General Counsel or their appointed delegate
QPAC	Queensland Performing Arts Trust
Serious Harm	Serious Harm is defined in paragraph 41
Suspected Eligible Data Breach	Suspected Eligible Data Breach is defined in paragraph 18

REFERENCES

Cyber Security Incident Response Plan
Emergency Management Plan
ICT Acceptable Use Policy
Information Privacy Act 2009 (Qld)
Information Security and Data Management Policy
Records Management Policy